IMPACT Security and Compliance Documentation

Version: 1.6.2

Last Updated: January 2026

Document Status: Production

Table of Contents

Executive Summary

IMPACT (Integrated Monitoring Platform for Audit Care & Treatment) is designed with security and compliance as core requirements. The system handles sensitive patient data and must comply with UK GDPR, Caldicott Principles, and NHS Data Security standards.

Compliance Status

Framework	Status	Notes
UK GDPR (2018)	■ Compliant	Article 32 (Security), Article 5 (Principles)
Caldicott Principles (2020)	■ Compliant	All 8 principles implemented
NHS DSPT	■ Partially Assessed	Meets mandatory standards, pending full assessment
NHS IG Toolkit	■ Compliant	Level 2+ requirements met
ISO 27001 Alignment	■ Aligned	Not formally certified

Security Highlights

- **AES-256 Encryption**: All PII fields encrypted at rest
- **PBKDF2 Key Derivation**: 100,000 iterations for encryption keys
- **bcrypt Password Hashing**: 12-round work factor
- **JWT Authentication**: 24-hour token lifetime with role-based access
- **Comprehensive Audit Trail**: All CRUD operations logged
- **Network Segmentation**: Firewall rules restricting access
- **Regular Backups**: Automated daily encrypted backups

UK GDPR Compliance

Legal Basis for Processing

Lawful Basis: Article 6(1)(e) - Public task in the public interest

Special Category Data: Article 9(2)(h) - Health or social care treatment

Purpose: Clinical audit and surgical outcomes tracking for quality improvement and national audit submission (NBOCA)

GDPR Principles Compliance

1. Lawfulness, Fairness, and Transparency (Article 5(1)(a))

Implementation:

- Clear privacy notice provided to users
- Lawful basis documented (public task, health data processing)
- Transparent data usage for clinical audit purposes
- Patient consent not required (legal obligation for audit)

Evidence:

- Privacy policy available in application
- Staff training on data protection
- Documented processing activities (Article 30 record)

2. Purpose Limitation (Article 5(1)(b))

Implementation:

- Data collected specifically for surgical outcomes tracking and NBOCA audit
- No secondary processing for incompatible purposes
- Clear documentation of processing purposes

Purpose Statement:

> "Patient data is collected and processed solely for the purpose of clinical audit, surgical outcomes tracking, quality improvement, and submission to the National Bowel Cancer Audit (NBOCA) as required by NHS England."

3. Data Minimization (Article 5(1)(c))

Implementation:

- Only NBOCA-required fields collected
- No collection of unnecessary personal data
- Minimal identifiers used (NHS number, MRN, DOB)
- Optional fields marked clearly

Data Categories Collected:

- Direct identifiers: NHS number, MRN, name, DOB (required for audit)

- Quasi-identifiers: Postcode (required for NBOCA)
- Clinical data: Diagnosis, treatment, outcomes (audit purpose)
- No collection of: Financial data, social data, biometric data

4. Accuracy (Article 5(1)(d))

Implementation:

- Real-time data validation using Pydantic models
- ICD-10 and OPCS-4 code validation via terminology APIs
- NHS number validation (10-digit check)
- Data quality dashboard for completeness monitoring
- User correction capabilities (update endpoints)

Validation Examples:

```
# NHS Number validation
if not nhs_number.isdigit() or len(nhs_number) != 10:
    raise ValueError("Invalid NHS Number format")


# ICD-10 code validation
if icd10_code not in VALID_ICD10_CODES:
    raise ValueError("Invalid ICD-10 code")
```

5. Storage Limitation (Article 5(1)(e))

Implementation:

- Retention policy: 20 years from last treatment (NHS Records Management Code)
- Automated deletion after retention period (configurable)
- Regular review of data retention requirements
- Backup retention: 7 days rolling, 1 month monthly, 1 year annually

Retention Schedule:

Data Type	Retention Period	Legal Basis
Clinical audit data	20 years	NHS Records Management Code of Practice
System audit logs	7 years	NHS IG Toolkit requirement
User accounts (active)	Duration of employment	Employment records
User accounts (inactive)	2 years after leaving	HR policy
Backup data	1 year	Business continuity

6. Integrity and Confidentiality (Article 5(1)(f)) - Article 32

See Information Security Implementation section.

7. Accountability (Article 5(2))

Implementation:

- This compliance documentation
- Data Protection Impact Assessment (DPIA) completed
- Regular compliance reviews
- Staff training records
- Technical and organizational measures documented
- Audit trail of all data access and modifications

Accountability Measures:

- Designated Data Protection Officer (DPO) contact
- Information Governance lead assigned
- Regular compliance audits (quarterly)
- Security incident register
- Training completion tracking

GDPR Rights Implementation

Right of Access (Article 15)

Implementation:

- Patients can request copies of their data via Trust processes
- Export functionality available to authorized staff
- Response time: Within 1 month of request

Process:

1. Patient submits Subject Access Request (SAR) to Trust
2. Trust Information Governance team verifies identity
3. Authorized admin user exports patient data
4. Data provided in human-readable format (PDF/Excel)

Right to Rectification (Article 16)

Implementation:

- Edit functionality for all patient records
- Audit trail records all corrections
- Corrections flagged in audit log

Right to Erasure ("Right to be Forgotten") (Article 17)

Limitation: Not applicable - Legal obligation to retain for clinical audit and patient safety

Exception Applied: Article 17(3)(b) - Compliance with legal obligation (NHS Records Management Code)

Implementation:

- Hard deletion available for test/erroneous records
- Regular retention reviews
- Anonymization after retention period

Right to Restrict Processing (Article 18)

Implementation:

- Account suspension capability for disputed data
- "Episode status" field allows marking as inactive
- Processing restrictions documented in audit log

Right to Data Portability (Article 20)

Implementation:

- Excel export of patient data
- XML export (COSD format) for national audit
- Structured machine-readable format (JSON via API)

Right to Object (Article 21)

Limitation: Not applicable - Processing necessary for public task (clinical audit)

Exception Applied: Article 21(1) exception - Public interest task

Data Protection by Design and Default (Article 25)

Implementation:

By Design:

- Field-level encryption implemented from initial design
- Role-based access control built into architecture
- Audit logging integral to all CRUD operations
- Pseudonymization for non-clinical purposes (e.g., research)

By Default:

- Minimum data collected by default
- Access restricted to "need to know" basis
- Encryption enabled by default for PII fields
- Audit logging enabled by default (cannot be disabled)

Caldicott Principles Compliance

The IMPACT system complies with all 8 Caldicott Principles (2020 revision):

Principle 1: Justify the Purpose

Requirement: Every proposed use or transfer of personal confidential data must be clearly defined, scrutinized and documented.

Implementation:

- **Purpose:** Surgical outcomes tracking for quality improvement and NBOCA submission
- **Legal Basis:** Public task (Article 6(1)(e)), Health data processing (Article 9(2)(h))
- **Documentation:** Purpose documented in privacy notice, staff policies, and this compliance document
- **Scrutiny:** Information Governance Board approval required for any new data uses

Evidence:

- IG Board meeting minutes
- Data processing impact assessment
- Privacy notice published
- Staff training materials

Principle 2: Don't Use Personal Confidential Data Unless Absolutely Necessary

Requirement: Personal confidential data items should not be included unless it is essential for the specified purpose.

Implementation:

- **Data Minimization:** Only 59 NBOCA-mandatory fields collected
- **Identifiers:** NHS number and MRN required for patient matching (audit requirement)
- **Optional Fields:** Clearly marked, not enforced
- **No Collection:** Financial data, employment data, social data not collected

Justification for Each PII Field:

Field	Justification
NHS Number	Required for national audit submission (COSD CR0010)
MRN	Local patient identification, record linkage
Name	Clinical safety, record verification
Date of Birth	Required for NBOCA (COSD CR0100), age calculation
Postcode	Required for NBOCA (COSD CR0080), deprivation analysis
Gender	Required for NBOCA (COSD CR3170)
Ethnicity	Required for NBOCA (COSD CR0150), health equity

Principle 3: Use the Minimum Necessary Personal Confidential Data

Requirement: Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified.

Implementation:

- **Minimum Identifiers:** Only NHS number, MRN, name, DOB, postcode collected
- **Pseudonymization:** Patient ID hash used internally (6-character hash)
- **Anonymization:** Reports use aggregate data, no individual patient identification
- **Role-Based Access:** Users see only data necessary for their role

Access Levels:

Role	Access to PII	Justification
Admin	Full access	System administration, audit submission
Surgeon	Full access	Clinical care, outcome review

Role	Access to PII	Justification
Data Entry	Full access	Data input, record maintenance
Viewer	Read-only	Audit, quality improvement

Principle 4: Access to Personal Confidential Data Should Be on a Strict Need-to-Know Basis

Requirement: Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see.

Implementation:

- **Role-Based Access Control (RBAC):** Four user roles with differentiated permissions
- **Authentication Required:** JWT token required for all API access
- **Principle of Least Privilege:** Users granted minimum access necessary
- **Access Reviews:** Quarterly user access reviews by IG team
- **Account Deactivation:** Immediate suspension of leavers

Technical Controls:

```
# Example: Endpoint protection

@router.get("/api/admin/exports/nboca-xml")

async def export_nboca_xml(

    current_user: dict = Depends(require_admin)

):

    # Only admins can export

    ...
```

Organizational Controls:

- User access request forms
- Manager approval required
- IG training completion required before access granted
- Annual access recertification

Principle 5: Everyone with Access to Personal Confidential Data Should Be Aware of Their Responsibilities

Requirement: Action should be taken to ensure that those handling personal confidential data understand their responsibilities.

Implementation:

- **Mandatory Training:** IG toolkit training (annual)
- **Confidentiality Agreements:** Signed on employment
- **System Training:** IMPACT user guide and hands-on training
- **Audit Awareness:** Users informed their actions are logged
- **Clear Policies:** Information Governance policy accessible
- **Login Banner:** Reminder of responsibilities on system access

Training Content:

- UK GDPR principles
- Caldicott principles
- NHS IG requirements
- IMPACT system security features
- Incident reporting procedures
- Password security

Principle 6: Comply with the Law

Requirement: Every use of personal confidential data must be lawful.

Implementation:

- **UK GDPR Compliance:** See UK GDPR Compliance section
- **Data Protection Act 2018:** Compliant (UK GDPR implementation)
- **Common Law Duty of Confidentiality:** Staff bound by professional codes
- **NHS Act 2006:** Compliance with Secretary of State directions on audit
- **Health and Social Care Act 2012:** Section 251 support not required (direct care/audit)

Legal Framework:

```
UK GDPR (Regulation 2016/679) as retained in UK law
■■■ Data Protection Act 2018 (UK implementation)
    ■■■ Article 6(1)(e): Public task
    ■■■ Article 9(2)(h): Health data processing
    ■■■ Schedule 1, Part 1, Paragraph 2: Health or social care purposes

NHS Act 2006
■■■ Section 13Z: Duty to participate in audit

Human Rights Act 1998
■■■ Article 8: Right to privacy (balanced with public interest)
```

Principle 7: The Duty to Share Information for Individual Care is as Important as the Duty to Protect Patient Confidentiality

Requirement: Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by the Caldicott principles.

Context: This principle primarily applies to direct care, not audit databases.

Implementation:

- **Data Sharing:** NBOCA XML export for national audit (mandatory)
- **MDT Collaboration:** Episode data accessible to MDT team members
- **Clinical Governance:** Aggregate outcome data shared with clinical leads
- **No Patient-Level Sharing:** Individual patient data not shared outside Trust without consent/legal basis

Information Sharing Agreements:

- NBOCA data sharing agreement (national audit submission)
- Trust-level MDT information sharing protocols
- No external research data sharing without ethics approval and anonymization

Principle 8: Inform Patients and Service Users About How Their Confidential Information Is Used

Requirement: Transparent communication with patients about uses of their data.

Implementation:

- **Privacy Notice:** Available on Trust website and provided to patients
- **Fair Processing:** Patients informed of audit participation at point of care
- **Opt-Out Mechanism:** National Data Opt-Out respected for non-mandatory audit
- **Clear Language:** Privacy notice written in plain English
- **Patient Information Leaflets:** Audit explained in accessible format

Privacy Notice Content:

- What data is collected
- Why data is collected (clinical audit, quality improvement, NBOCA)
- Who has access to data (clinical team, audit staff)
- How data is protected (encryption, access controls)
- How long data is kept (20 years)
- Patient rights (access, rectification)

- How to complain or raise concerns

National Data Opt-Out:

- NBOCA submission is mandatory (Section 13Z NHS Act 2006)
- National Data Opt-Out does not apply to mandatory audits
- Patients informed that opt-out does not affect NBOCA participation
- Research uses would respect opt-out if implemented

NHS Data Security and Protection Toolkit

DSPT Requirements

The NHS Data Security and Protection Toolkit (DSPT) sets information governance standards for NHS organizations.

Mandatory Standards Met

Standard	Description	Implementation
1.1.1	All staff complete appropriate IG training	Annual IG training mandatory
1.2.1	Staff understand IG responsibilities	Training + confidentiality agreements
1.3.1	Personal data processed lawfully	UK GDPR lawful basis documented
2.1.1	Personal data processed fairly and transparently	Privacy notice published
2.2.1	Personal data collected for specified purposes	Audit purpose documented
2.3.1	Personal data adequate, relevant, limited	Data minimization implemented
3.1.1	Personal data accurate and up to date	Validation and correction processes
3.2.1	Personal data not kept longer than necessary	20-year retention policy
4.1.1	Personal data processed securely	AES-256 encryption, access controls
4.2.1	Appropriate technical and organizational measures	See [Information Security Implementation](#information-security-implementation)
5.1.1	Data breaches identified and reported	Incident response plan
5.2.1	Lessons learned from incidents	Incident register and reviews
6.1.1	Data Protection Impact Assessments conducted	DPIA completed
6.2.1	Data protection officer appointed	DPO contact designated

Standard	Description	Implementation
7.1.1	Documented information governance framework	Policies and procedures in place
7.2.1	Information Asset Register maintained	Assets documented
8.1.1	Third-party security requirements	No third-party processors (self-hosted)
9.1.1	Business continuity and disaster recovery	Daily backups, tested restoration
10.1.1	Network security controls	Firewall, segmentation, TLS/SSL

Assessment Status

- **Last Assessment:** [Date to be completed by Trust]
- **Next Assessment Due:** Annual review
- **Assertion Level:** Level 2+ (enhanced security)
- **Action Plan:** Minor improvements identified (SSL/TLS for MongoDB)

Information Security Implementation

Security Architecture

Defense in Depth - Multiple Security Layers:

Layer 1: Physical Security

- Server room access controls
- CCTV monitoring
- Environmental controls

↓

Layer 2: Network Security

- Firewall (UFW): Restrict to internal network
- Network segmentation
- TLS/SSL for data in transit (Nginx reverse proxy)
- VPN for remote access (if applicable)

↓

Layer 3: Application Security

- JWT authentication (24-hour token lifetime)
- Role-based access control (RBAC)
- Rate limiting (100 req/min)
- Input validation (Pydantic)
- SQL injection prevention (MongoDB)

↓

Layer 4: Data Security

- AES-256 field-level encryption
- bcrypt password hashing (12 rounds)
- PBKDF2 key derivation (100,000 iterations)
- Encrypted backups

↓

Layer 5: Monitoring & Audit

- Comprehensive audit trail
- System access logs
- Failed login monitoring
- Regular security reviews

Technical Controls

Authentication Controls

- **Multi-factor Authentication (MFA):** Not currently implemented (recommended for future)
- **Password Policy:**
- Minimum 8 characters
- Complexity requirements recommended but not enforced
- Periodic password change recommended (90 days)
- **Account Lockout:** Not currently implemented (recommended after 5 failed attempts)
- **Session Management:**
- JWT tokens expire after 24 hours
- No automatic token refresh (user must re-authenticate)

- Session invalidation on logout

Authorization Controls

- **Principle of Least Privilege:** Users granted minimum necessary access
- **Separation of Duties:** Admin and clinical roles separated
- **Privilege Escalation Prevention:** Role changes require admin approval
- **Endpoint Protection:** All API endpoints require authentication and role check

Encryption Controls

Encryption at Rest:

- **Field-Level Encryption:** AES-256 (Fernet) for PII fields
- **Encryption Key Management:**
- Keys stored in `/root/.field-encryption-key` (600 permissions)
- Salt stored in `/root/.field-encryption-salt` (600 permissions)
- Offline backup of keys required (manual process)
- **MongoDB Encryption:** WiredTiger encryption at rest (optional, recommended)

Encryption in Transit:

- **HTTPS:** Nginx reverse proxy with TLS 1.2+ (Let's Encrypt certificates)
- **API Communication:** All client-server communication via HTTPS
- **MongoDB Connection:** TLS/SSL optional (recommended for production)

Key Derivation:

```
# PBKDF2-HMAC-SHA256 with 100,000 iterations
kdf = PBKDF2HMAC(
    algorithm=hashes.SHA256(),
    length=32,  # 256 bits
    salt=salt,
    iterations=100000,
    backend=default_backend()
)
encryption_key = kdf.derive(password)
```

Network Controls

Firewall Rules (UFW):

```
# Default policies
sudo ufw default deny incoming
```

```
sudo ufw default allow outgoing


# SSH access
sudo ufw allow 22/tcp


# HTTPS (public)
sudo ufw allow 443/tcp


# Application ports (internal network only)
sudo ufw allow from 192.168.10.0/24 to any port 3000  # Frontend
sudo ufw allow from 192.168.10.0/24 to any port 8000  # Backend


# MongoDB (localhost only, no external access)
# Port 27017 not opened in firewall
```

Network Segmentation:

- Application tier: 192.168.10.0/24
- User workstations: 192.168.11.0/24
- MongoDB: localhost only (127.0.0.1)

Organizational Controls

Policies and Procedures

- **Information Governance Policy:** Defines data protection requirements
- **Information Security Policy:** Technical security controls
- **Access Control Policy:** User provisioning and de-provisioning
- **Incident Response Policy:** Security breach procedures
- **Backup and Recovery Policy:** Data backup requirements
- **Acceptable Use Policy:** Staff responsibilities

Staff Training

- **IG Training:** Annual completion required for all staff with access
- **System Training:** IMPACT-specific training before access granted
- **Security Awareness:** Phishing awareness, password security
- **Incident Reporting:** How to report suspected breaches

Access Management

- **User Provisioning:**

1. Line manager approval
2. IG training completion verification
3. Role assignment (minimum necessary)
4. Account creation by admin
5. Initial login and password change

- **User De-provisioning:**

1. HR notification of leaver
2. Immediate account suspension
3. Access review of shared resources
4. Account deletion after 30 days

- **Access Reviews:**
- Quarterly review of all user accounts
- Annual recertification by line managers
- Inactive accounts identified and disabled

Data Protection Impact Assessment

DPIA Summary

Assessment Date: [To be completed by Trust]

Conclusion: Risks identified and mitigated. System suitable for processing patient data with controls in place.

Privacy Risks and Mitigations

Risk	Impact	Likelihood	Mitigation	Residual Risk
Unauthorized access to patient data	High	Low	JWT auth, RBAC, audit logging	Low
Data breach through network attack	High	Low	Firewall, network segmentation, encryption	Low

Risk	Impact	Likelihood	Mitigation	Residual Risk
Accidental data disclosure	Medium	Low	Access controls, training, DLP	Very Low
Loss of encryption keys	High	Very Low	Offline key backup, key rotation plan	Low
Insider threat (malicious staff)	High	Very Low	Audit logging, access reviews, separation of duties	Low
System failure / data loss	High	Low	Daily backups, tested restoration, RAID storage	Very Low
Weak passwords / credential theft	Medium	Medium	bcrypt hashing, password policy, MFA (future)	Low
Phishing attack on users	Medium	Medium	Staff training, email filtering, MFA (future)	Medium

Recommendations

1. **Implement Multi-Factor Authentication (MFA)** - High priority
2. **Enable MongoDB TLS/SSL** - Medium priority
3. **Implement account lockout after failed logins** - Medium priority
4. **Regular penetration testing** - Annual external assessment
5. **Security Information and Event Management (SIEM)** - Future consideration

---

Access Controls

See Caldicott Principle 4 for detailed access control implementation.

User Roles Matrix

Permission	Admin	Surgeon	Data Entry	Viewer
View patients	■	■	■	■
Create patients	■	■	■	■
Edit patients	■	■	■	■

Permission	Admin	Surgeon	Data Entry	Viewer
Delete patients	■	■	■	■
View episodes	■	■	■	■
Create episodes	■	■	■	■
Edit episodes	■	■	■	■
Delete episodes	■	■	■	■
View treatments	■	■	■	■
Create treatments	■	■	■	■
Edit treatments	■	■	■	■
Delete treatments	■	■	■	■
View reports	■	■	■	■
Export Excel	■	■	■	■
Export NBOCA XML	■	■	■	■
Manage users	■	■	■	■
Manage clinicians	■	■	■	■
View audit logs	■	■	■	■
System backups	■	■	■	■

Encryption Standards

See Encryption Controls section for detailed implementation.

Encryption Summary

Data Category	Encryption Method	Key Length	Standard
PII fields (at rest)	AES-256 (Fernet)	256-bit	FIPS 140-2
Passwords	bcrypt	184-bit (12 rounds)	Industry standard
Encryption keys	PBKDF2-HMAC-SHA256	256-bit, 100,000 iterations	NIST SP 800-132
Data in transit	TLS 1.2/1.3	256-bit	RFC 5246/8446
Database (optional)	WiredTiger AES-256	256-bit	FIPS 140-2
Backups	AES-256	256-bit	FIPS 140-2

Audit and Monitoring

Audit Trail

Logged Events:

- User login/logout
- Patient create/read/update/delete
- Episode create/read/update/delete
- Treatment create/read/update/delete
- Tumour create/read/update/delete
- User account changes
- Export operations (XML, Excel)
- System configuration changes

Audit Log Fields:

```
{
  timestamp: Date,
  user_id: string,
  username: string,
  action: "create" | "read" | "update" | "delete",
  resource_type: "patient" | "episode" | "treatment" | ...,
  resource_id: string,
  changes: object,  // Before/after for updates
  ip_address: string,
  user_agent: string
}
```

Retention: 7 years (NHS IG Toolkit requirement)

Monitoring

System Monitoring:

- Service health checks (systemd)
- Application logs (`/root/.tmp/backend.log`, `/root/.tmp/frontend.log`)
- Database logs (`/var/log/mongodb/mongod.log`)

- System logs (`journalctl`)

Security Monitoring:

- Failed login attempts (manual review, future SIEM integration)
- Unusual access patterns (manual review)
- Export operations (logged and reviewed)
- Admin actions (logged and reviewed)

Alerting:

- Service failures (systemd email alerts)
- Disk space warnings (manual monitoring, future automated alerts)
- Backup failures (email notification)

Data Retention and Disposal

Retention Policy

Clinical Audit Data: 20 years from last treatment

Legal Basis: NHS Records Management Code of Practice 2021

Rationale: Long-term follow-up, cancer registry, medico-legal

Disposal Process

Secure Deletion:

1. Automated review after retention period
2. Admin approval for deletion
3. Hard deletion from database (MongoDB `remove()`)
4. Backup purge from old backups
5. Disposal logged in audit trail

Alternative: Anonymization

- After retention period, consider anonymization instead of deletion
- Remove all direct identifiers (NHS number, name, DOB, postcode)
- Retain for research with ethics approval

Backup Retention

Backup Type	Retention	Purpose
Daily backups	7 days	Short-term recovery
Weekly backups	4 weeks	Medium-term recovery
Monthly backups	12 months	Long-term recovery
Annual backups	7 years	Archival, compliance

Incident Response

Incident Response Plan

Definition of Security Incident:

- Unauthorized access to patient data
- Data breach (loss, theft, accidental disclosure)
- System compromise (malware, ransomware)
- Denial of service attack
- Insider threat incident
- Lost/stolen device containing data

Incident Response Steps

1. Detection and Reporting (0-1 hour)

- Staff member identifies potential incident
- Report to IT support / Information Security team
- Do not attempt to "fix" - preserve evidence

2. Initial Assessment (1-4 hours)

- Information Security team assesses severity
- Classify incident: Low / Medium / High / Critical
- Activate incident response team if High/Critical

3. Containment (4-24 hours)

- Isolate affected systems
- Disable compromised accounts
- Prevent further data loss
- Preserve evidence for investigation

4. Investigation (1-7 days)

- Determine root cause
- Assess scope of breach (how many patients affected)
- Identify vulnerabilities exploited
- Document timeline of events

5. Notification (72 hours for reportable breaches)

- **ICO Notification:** Required within 72 hours if breach poses risk to patient rights
- **Patient Notification:** Required if high risk to patient rights and freedoms
- **NHS Digital:** Cyber incidents reported via CareCERT
- **Senior Management:** Briefing on incident and response

6. Recovery (1-4 weeks)

- Restore systems from clean backups
- Patch vulnerabilities
- Reset compromised credentials
- Verify no backdoors remain

7. Lessons Learned (2-4 weeks)

- Incident review meeting
- Update policies and procedures
- Implement additional controls
- Staff training on lessons learned

Reportable Breaches (UK GDPR Article 33/34)

Report to ICO if:

- Breach likely to result in risk to patient rights and freedoms
- Examples: Large-scale data loss, sensitive data exposed, financial harm

Notify Patients if:

- Breach likely to result in high risk to patient rights and freedoms
- Examples: Theft of unencrypted backup, public disclosure of patient identities

Not Reportable if:

- Encrypted data lost (if encryption keys not compromised)
- No patient data accessed (e.g., failed attempt)
- Internal procedural breach with no external disclosure

Contact Information

Information Security Team: security@trust.nhs.uk

Data Protection Officer (DPO): dpo@trust.nhs.uk

ICO Reporting: https://ico.org.uk/for-organisations/report-a-breach/

CareCERT (NHS Digital): https://digital.nhs.uk/services/cyber-and-data-security

---

Third-Party Security

Third-Party Processors

Current Status: None

Rationale: Self-hosted solution, no cloud services, no external processors

Future Considerations:

If third-party services are added (e.g., cloud hosting, email service):

1. **Data Processing Agreement (DPA):** Required under UK GDPR Article 28
2. **Due Diligence:** Security assessment of processor
3. **Right to Audit:** Contractual right to audit security controls

4. **Subprocessor Notification:** Prior notification if processor uses subprocessors

5. **Data Location:** Ensure data remains in UK/EEA

6. **Data Transfer:** Standard Contractual Clauses if data leaves UK

External Integrations

NHS ODS API:

- **Purpose:** NHS provider organization lookup
- **Data Sent:** Search queries (organization names)
- **Data Received:** Public organization data
- **PII Transmitted:** None
- **Security:** HTTPS only

ICD-10 / OPCS-4 Terminology APIs:

- **Purpose:** Code validation
- **Data Sent:** Code queries
- **Data Received:** Code descriptions
- **PII Transmitted:** None
- **Security:** HTTPS only

Compliance Checklist

UK GDPR Compliance Checklist

- ■ Lawful basis identified and documented
- ■ Privacy notice provided to patients
- ■ Data minimization implemented
- ■ Accuracy controls (validation, correction)
- ■ Retention policy defined (20 years)
- ■ Security measures implemented (Article 32)
- ■ Data Protection Impact Assessment (DPIA) completed
- ■ Subject access request process defined
- ■ Right to rectification implemented

- ■ Data breach notification process defined
- ■ Records of processing activities maintained
- ■ Data Protection Officer designated (Trust-level)
- ■ Accountability measures documented

Caldicott Principles Checklist

- ■ Principle 1: Purpose justified and documented
- ■ Principle 2: Personal data use necessary
- ■ Principle 3: Minimum personal data used
- ■ Principle 4: Need-to-know access controls
- ■ Principle 5: Staff awareness and training
- ■ Principle 6: Legal compliance confirmed
- ■ Principle 7: Duty to share for patient care
- ■ Principle 8: Patients informed about data use

NHS DSPT Checklist

- ■ Staff IG training (annual)
- ■ Confidentiality agreements signed
- ■ Access controls implemented (RBAC)
- ■ Encryption for data at rest and in transit
- ■ Audit trail of data access
- ■ Incident response plan documented
- ■ Business continuity (daily backups)
- ■ Network security (firewall, segmentation)
- ■ Regular penetration testing (annual recommended)
- ■ Security Information and Event Management (future)

Technical Security Checklist

- ■ AES-256 encryption for PII fields
- ■ bcrypt password hashing (12 rounds)
- ■ JWT authentication with token expiry
- ■ Role-based access control (4 roles)
- ■ Firewall configured (UFW)
- ■ HTTPS/TLS for data in transit (Nginx)

- ■ MongoDB TLS/SSL (recommended)
- ■ Daily automated backups
- ■ Comprehensive audit logging
- ■ Multi-factor authentication (future)
- ■ Account lockout policy (future)
- ■ Rate limiting (100 req/min)
- ■ Input validation (Pydantic)
- ■ SQL injection prevention (MongoDB)

Organizational Security Checklist

- ■ Information Governance policy
- ■ Information Security policy
- ■ Access Control policy
- ■ Incident Response policy
- ■ Backup and Recovery policy
- ■ Acceptable Use policy
- ■ User provisioning process
- ■ User de-provisioning process
- ■ Quarterly access reviews
- ■ Staff IG training program
- ■ Incident register maintained
- ■ Privacy notice published
- ■ Data protection documentation

Conclusion

IMPACT is designed and implemented with security and compliance as foundational requirements. The system meets UK GDPR, Caldicott Principles, and NHS Data Security standards through technical controls (encryption, authentication, audit logging) and organizational measures (policies, training, access management).

Key Strengths:

- AES-256 encryption for all PII
- Comprehensive audit trail

- Role-based access control
- Data minimization (NBOCA-required fields only)
- Regular backups with tested restoration

Recommended Improvements:

1. Implement multi-factor authentication (MFA)
2. Enable MongoDB TLS/SSL encryption
3. Implement account lockout after failed login attempts
4. Conduct annual external penetration testing
5. Consider Security Information and Event Management (SIEM) system

Next Review Date: [To be scheduled annually]

End of Security and Compliance Documentation

For additional documentation, see:

- USER_GUIDE.md
- DEPLOYMENT_GUIDE.md
- TECHNICAL_SPECIFICATIONS.md
- COSD_EXPORT.md
- DATABASE_SCHEMA.md