SolGuruz

Healthcare CRM Security and Compliance Checklist

2026 Edition

Use this checklist to verify your healthcare CRM meets security, compliance, and interoperability standards before launch and at every compliance review cycle. Tick each item once verified. Items marked are newly mandatory under the 2026 HIPAA Rule updates.

Section 1: Security Protocols

1.1 Business Associate Agreement (BAA)

- ☐ Signed BAA in place with all vendors, cloud providers, and subprocessors that handle PHI
- ☐ BAA covers all downstream subprocessors in your infrastructure chain
- ☐ BAA reviewed and updated within the last 12 months
- ☐ BAA includes breach notification timelines, permissible uses, and data return and destruction provisions

1.2 Data Encryption

Both items below are now explicitly mandatory under the 2026 HIPAA Rule updates.

- ☐ **Data at rest:** AES-256 encryption applied to all databases, backup drives, and server storage
- ☐ **Data in transit:** TLS 1.3 encryption applied to all data moving between devices, networks, and servers
- ☐ Encryption keys managed securely with rotation policy in place
- ☐ Encrypted backups tested for restoration integrity quarterly

1.3 Role-Based Access Control (RBAC)

- ☐ Access permissions defined by clinical role before system launch
- ☐ Clinical staff can only access records relevant to their specific function
- ☐ Billing administrators have no access to clinical notes or treatment records
- ☐ Channel partners and external users have separate, restricted permission sets
- ☐ RBAC permissions reviewed and updated when staff roles change

1.4 Multi-Factor Authentication (MFA)

MFA is now a required control for all systems accessing ePHI under the 2026 HIPAA Rule updates.

- ☐ MFA enabled for all user accounts accessing electronic PHI (ePHI)
- ☐ MFA required for all admin accounts without exception
- ☐ MFA covers all access pathways including mobile, web, and API access

1.5 Telehealth and Remote Access Security

- ☐ All remote access pathways secured through encrypted VPN tunnels
- ☐ Device authentication required for all remote CRM access
- ☐ Session timeout controls configured to match HIPAA remote access standards
- ☐ Mobile CRM access requires device-level authentication and encryption

1.6 Audit Trails and Continuous Monitoring

- ☐ Immutable audit trail captures every access event, record view, data modification, and export
- ☐ Audit logs retained for minimum 6 years as required by HIPAA
- ☐ Real-time monitoring in place to detect anomalous access patterns
- ☐ Alerts configured for unusual access volume, off-hours access, and bulk data exports
- ☐ Audit logs reviewed regularly by designated security personnel

1.7 Security Audits and Penetration Testing

All three items below are now required compliance activities under the 2026 HIPAA Rule updates.

- ☐ Annual penetration testing scheduled and documented
- ☐ Biannual vulnerability scans completed and results documented
- ☐ Quarterly backup restoration tests completed and passed
- ☐ All identified vulnerabilities have documented remediation timelines
- ☐ Security findings reviewed by senior technical lead before sign-off

1.8 Patient Consent Management

- ☐ Consent capture workflow implemented at point of data collection
- ☐ Patients can view, update, and withdraw consent through a documented process
- ☐ Consent records are retrievable and auditable for any patient relationship
- ☐ Communication channel preferences captured and honoured
- ☐ Data processing records document what each patient consented to and when

1.9 Staff Training and Data Security Culture

- ☐ Role-specific security training programme documented and delivered to all staff with PHI access
- ☐ Phishing awareness training completed annually by all clinical and administrative staff
- ☐ Incident reporting procedure clearly communicated to all staff
- ☐ Acceptable use policy signed by all staff with CRM access
- ☐ Training records maintained for compliance audit purposes

Section 2: Compliance Requirements by Country

Check every jurisdiction where your patients are located. Each country has distinct compliance obligations that must be designed into your CRM architecture.

- ☐ **USA:** *HIPAA*, *HITECH Act*, *HITRUST CSF*
  Requirements: PHI encryption, breach notification, BAA, MFA, audit trails, 2026 Rule updates

- ☐ **EU (All 27 Member States):** *GDPR*, *EU AI Act (from August 2026)*, *European Health Data Space (EHDS)*
  Requirements: Explicit consent, data residency, right to erasure, DPA with all processors, AI risk assessment

- ☐ **UK:** *UK GDPR*, *NHS Data Security and Protection Toolkit (DSPT)*
  Requirements: Annual DSPT submission, staff training evidence, data security policies, cyber resilience

- ☐ **India:** *DPDP Act 2023*, *ABDM Framework*
  Requirements: Consent-based processing, CERT-In 6-hour breach reporting, 180-day log retention

- ☐ **UAE:** *Federal Law No. 2 of 2019*, *PDPL*
  Requirements: 25-year data retention, data localisation, no transfer outside UAE without regulatory approval

- ☐ **Australia:** *My Health Records Act 2012*, *Privacy Act 1988*
  Requirements: Breach notification, Australian Privacy Principles, IRAP for government health data

- ☐ **Canada:** *PIPEDA*, *PHIPA* / *HIPA* *(provincial)*
  Requirements: Provincial law compliance, consent, access rights based on operating province

- ☐ **Germany:** *GDPR*, *SGB V*, *§203 StGB*
  Requirements: German-controlled encryption keys, data residency, BSI C5 for cloud providers

- ☐ **Singapore:** *PDPA*, *Healthcare Services Act 2020*
  Requirements: MOH IT security guidelines, explicit consent, breach notification, MAS TRM

- ☐ **Kuwait:** *CITRA DPPR No. 26 of 2024*
  Requirements: 24-hour breach notification, consent, cross-border transfer restrictions

- ☐ **Saudi Arabia:** *PDPL 2021 (amended 2023)*, *NCA ECC*
  Requirements: NCA cybersecurity controls, SAMA framework for health insurance entities

- ☐ **South Africa:** *POPIA 2013*
  Requirements: Information Officer appointed, breach notification to regulator, special data consent

- ☐ **Netherlands:** *GDPR*, *WGBO (Medical Treatment Agreement Act)*
  Requirements: 20-year record retention, provider-controlled encryption keys, NEN 7510

- ☐ **Switzerland:** *nLPD (effective September 2023)*
  Requirements: DPIA for high-risk processing, data protection advisor, explicit consent for health data

- ☐ **Belgium:** *GDPR*, *Patient Rights Act*
  Requirements: Patient access rights, eHealth platform integration, GDPR Article 32 attestation

☐ **Hungary:** *GDPR, Act XLVII of 1997, EU AI Act (from August 2026)*
Requirements: Health data confidentiality rules, EU AI Act compliance for healthcare AI from August 2026

☐ **Hong Kong:** *Personal Data (Privacy) Ordinance (PDPO), Hospital Authority Patient Data Policy*
Requirements: Six Data Protection Principles, patient data governance policy compliance

Section 3: US Healthcare-Specific Legal Compliance

Required for platforms that touch Medicare or Medicaid workflows.

Anti-Kickback Statute (AKS)

- [ ] AKS exposure assessed for any pricing arrangement tied to referral activity
- [ ] Software discounts or bundled tools not contingent on Medicare or Medicaid referral volume
- [ ] Legal review completed for any referral management or EHR integration

Stark Law (Physician Self-Referral Law)

- [ ] Physician referral workflows documented to support Stark Law compliance
- [ ] Financial relationships between referring physicians and covered entities reviewed
- [ ] Referral tracking software architected to support Stark Law documentation

False Claims Act (FCA)

- [ ] Billing, coding, and claims workflows reviewed to prevent incorrect or inflated claims
- [ ] AI-assisted clinical documentation tools validated against upcoding risk
- [ ] Claims submission system includes validation logic before submission to CMS

Section 4: Industry Security Certifications

Check certifications relevant to your target markets and client procurement requirements.

- ☐ **SOC 2 Type II:** US enterprise clients, SaaS healthcare buyers, investor due diligence, global hospital procurement
- ☐ **ISO 27001:** UK NHS suppliers, EU healthcare clients, enterprise buyers in Germany, Netherlands, Belgium, Singapore, Australia
- ☐ **HITRUST CSF:** US health systems, insurers, and hospital groups requiring HIPAA assurance beyond a standard BAA
- ☐ **ISO 27701:** EU, UK, and Canadian markets handling cross-border health data, GDPR and PIPEDA compliance
- ☐ **GDPR Article 32 Compliance Attestation:** EU and UK hospital procurement, data protection officers, GDPR-regulated countries
- ☐ **Cyber Essentials Plus:** UK NHS suppliers, UK government healthcare contracts
- ☐ **BSI C5:** Cloud providers serving German healthcare organisations
- ☐ **NEN 7510:** Dutch healthcare IT vendor selection, Dutch hospitals and insurers
- ☐ **IRAP:** Australian government healthcare agencies, Medicare and My Health Records data
- ☐ **MAS TRM / MOH Healthcare IT Security Guidelines:** Singapore MOH-licensed healthcare providers and technology vendors
- ☐ **NCA ECC:** Saudi healthcare providers, government hospitals, health insurance companies
- ☐ **CERT-In Guidelines (India):** All healthcare IT platforms, EHR providers, and telemedicine companies in India

Section 5: Interoperability Standards

Verify your healthcare CRM supports the data exchange standards required for your clinical environment.

- ☐ **HL7 FHIR R4:** CRM integrates with EHR systems via FHIR R4 RESTful APIs. Required: US (21st Century Cures Act), UK, Australia, Canada, Germany, Singapore.
- ☐ **HL7 v2 / v3:** HL7 v2 messaging supported for lab results, admissions, and billing with legacy hospital infrastructure. Required globally for any CRM integrating with legacy systems.
- ☐ **DICOM:** Medical imaging data (X-rays, MRIs, CT scans) handled per DICOM standard. Required for any CRM with radiology or imaging integration.
- ☐ **SNOMED CT:** Clinical concepts represented in SNOMED CT terminology. Required: UK NHS, Australia, Canada, Singapore for clinical documentation.
- ☐ **ICD-10 / ICD-11:** Disease classification uses ICD-10 with ICD-11 migration plan. Required for all platforms with diagnosis coding, claims processing, or clinical reporting.
- ☐ **21st Century Cures Act (Information Blocking Rule):** FHIR-based API access enabled and information blocking policies documented. Required: US EHR vendors and ONC-certified systems.

Section 6: 2026 HIPAA Rule Updates: Action Required

The following items were previously optional or addressable. From late 2026, they are explicitly mandatory. All must be implemented and verifiable before the compliance deadline.

- ☐ Encryption at rest implemented with AES-256 (mandatory, no longer addressable)
- ☐ Encryption in transit implemented with TLS 1.3 (mandatory, no longer addressable)
- ☐ MFA enabled for all systems accessing ePHI (mandatory, no longer addressable)
- ☐ Annual penetration testing scheduled and documented
- ☐ Biannual vulnerability scans scheduled and documented
- ☐ Quarterly backup restoration tests completed, documented, and passed
- ☐ All technical safeguards verifiably implemented, not just documented in policy

Checklist produced by SolGuruz
HIPAA-Compliant Healthcare CRM Development
solguruz.com/crm/healthcare/