Contents

RADIANT Compliance Guide

Overview

This document outlines RADIANT's compliance posture for SOC 2, HIPAA, and GDPR requirements.

Compliance Matrix

Framework	Tier Required	Status
SOC 2 Type II	All tiers	Controls implemented
HIPAA	Tier 3+ (GROWTH)	BAA available
GDPR	All tiers (EU data)	DPA available
PCI DSS	N/A	Not applicable (no card data)

SOC 2 Controls

Trust Service Criteria

Security (Common Criteria)

Control	Implementation
CC1.1 - Board oversight	Documented security policies
CC2.1 - Communication	Security awareness training
CC3.1 - Risk assessment	Annual risk assessments
CC4.1 - Monitoring	CloudWatch, GuardDuty
CC5.1 - Logical access	IAM, Cognito, RLS
CC6.1 - System operations	Runbooks, on-call
CC7.1 - Change management	CI/CD, PR reviews
CC8.1 - Risk mitigation	WAF, rate limiting
CC9.1 - Entity risk	Vendor assessments

Availability

Control	Implementation
A1.1 - Capacity planning	Auto-scaling, monitoring
A1.2 - Environmental protection	Multi-AZ, DR procedures
A1.3 - Recovery	Backups, PITR, runbooks

Confidentiality

Control	Implementation
C1.1 - Data classification	PII tagging, encryption
C1.2 - Data disposal	Lifecycle policies

Evidence Collection

```
// Automated evidence collection
const auditLogs = {
  // All admin actions logged
  source: 'audit_logs table',
  retention: '7 years',

  // Access logs
  accessLogs: 'CloudWatch Logs',

  // Configuration changes
  configChanges: 'AWS Config',

  // Security events
  securityEvents: 'GuardDuty findings',
};
```

Annual Audit Checklist

- □ Access review completed
- □ Penetration test completed
- □ Vulnerability scan completed
- □ Security training completed
- □ Incident response test completed
- □ DR test completed
- □ Vendor assessments updated
- □ Policies reviewed and updated

HIPAA Compliance

Applicability

HIPAA compliance is available for Tier 3 (GROWTH) and above, which includes: - Encryption at rest (AES-256) - Encryption in transit (TLS 1.3) - Audit logging - Access controls - BAA with AWS

Technical Safeguards

Requirement	Implementation
Access Control (§164.312(a))	Cognito MFA, RLS, RBAC
Audit Controls (§164.312(b))	CloudTrail, audit_logs table
Integrity Controls (§164.312(c))	Checksums, versioning
Transmission Security (§164.312(e))	TLS 1.3, VPC endpoints

Administrative Safeguards

Requirement	Implementation
Security Officer	Designated in org
Workforce Training	Annual security training
Access Management	Quarterly access reviews
Incident Response	Documented procedures

Physical Safeguards

Handled by AWS: - Data center security - Device controls - Facility access

PHI Data Handling

```sql
-- PHI fields are encrypted at column level
CREATE TABLE patient_data (
  id UUID PRIMARY KEY,
  tenant_id UUID NOT NULL,
  -- PHI fields use additional encryption
  encrypted_data BYTEA NOT NULL,
  encryption_key_id VARCHAR(255) NOT NULL,
  created_at TIMESTAMPTZ DEFAULT NOW()
);

-- Enable RLS for tenant isolation
ALTER TABLE patient_data ENABLE ROW LEVEL SECURITY;
```

BAA Requirements

Before processing PHI: 1. Sign BAA with RADIANT 2. Enable HIPAA-eligible services only 3. Configure CloudTrail logging 4. Enable AWS Config 5. Review shared responsibility model

GDPR Compliance

Data Subject Rights

Right	Implementation
Right to Access	Data export API
Right to Rectification	Self-service + API
Right to Erasure	Deletion API + cascade
Right to Restrict	Processing flags
Right to Portability	JSON/CSV export
Right to Object	Consent management

Data Export (Right to Access)

```typescript
// API endpoint for data export
// GET /api/v2/gdpr/export
async function exportUserData(userId: string): Promise<UserDataExport> {
  return {
    personalData: await getPersonalData(userId),
    activityLogs: await getActivityLogs(userId),
    preferences: await getPreferences(userId),
    exportedAt: new Date().toISOString(),
    format: 'JSON',
  };
}
```

Data Deletion (Right to Erasure)

```
// API endpoint for data deletion
// DELETE /api/v2/gdpr/delete
async function deleteUserData(userId: string): Promise<DeletionResult> {
  // Cascade delete all user data
  await deletePersonalData(userId);
  await deleteActivityLogs(userId);
  await deletePreferences(userId);
  await deleteApiKeys(userId);

  // Anonymize audit logs (retain for compliance)
  await anonymizeAuditLogs(userId);

  return {
    deletedAt: new Date().toISOString(),
    confirmation: generateDeletionCertificate(userId),
  };
}
```

Data Processing Agreement

DPA includes: - Nature and purpose of processing - Types of personal data - Categories of data subjects - Sub-processor list - Technical measures - Audit rights

Data Residency

Region	Data Location	Backup Location
EU	eu-west-1 (Ireland)	eu-central-1 (Frankfurt)
US	us-east-1 (Virginia)	us-west-2 (Oregon)
APAC	ap-northeast-1 (Tokyo)	ap-southeast-1 (Singapore)

```
// Enforce data residency
const dataResidency = {
  EU: ['eu-west-1', 'eu-central-1'],
  US: ['us-east-1', 'us-west-2'],
  APAC: ['ap-northeast-1', 'ap-southeast-1'],
};

// Route requests to appropriate region
function routeByResidency(tenantRegion: string): string {
  return dataResidency[tenantRegion][0];
}
```

Consent Management

```
-- Consent tracking table
CREATE TABLE consent_records (
  id UUID PRIMARY KEY DEFAULT gen_random_uuid(),
  user_id UUID NOT NULL REFERENCES users(id),
  consent_type VARCHAR(50) NOT NULL,
  granted BOOLEAN NOT NULL,
  granted_at TIMESTAMPTZ,
  withdrawn_at TIMESTAMPTZ,
  ip_address INET,
  user_agent TEXT,
  created_at TIMESTAMPTZ DEFAULT NOW()
);

-- Consent types: marketing, analytics, essential, third_party
```

Data Classification

Classification Levels

Level	Description	Examples	Controls
Public	No restrictions	Marketing content	None
Internal	Business use	Metrics, configs	Access control
Confidential	Sensitive business	API keys, billing	Encryption, audit
Restricted	Highly sensitive	PHI, PII, credentials	Full controls

PII Fields

```
// Fields classified as PII
const piiFields = [
  'email',
  'display_name',
  'phone_number',
  'ip_address',
  'user_agent',
  'billing_address',
  'payment_method',
];

// Automatic PII detection and tagging
function tagPiiFields(data: Record<string, unknown>): void {
  for (const field of piiFields) {
    if (data[field]) {
      // Tag for audit and retention policies
      data[`${field}_pii`] = true;
    }
  }
}
```

Encryption

At Rest

Data Type	Encryption	Key Management
Database	AES-256	AWS KMS
S3	AES-256	AWS KMS
Secrets	AES-256	Secrets Manager
Backups	AES-256	AWS KMS

In Transit

Connection	Protocol	Minimum Version
API	TLS	1.2 (1.3 preferred)
Database	TLS	1.2
Internal	TLS	1.2

Key Rotation

```
// Automatic key rotation
const kmsKey = new kms.Key(this, 'Key', {
  enableKeyRotation: true,  // Annual rotation
  rotationPeriod: cdk.Duration.days(365),
});
```

Audit Logging

What We Log

Event Type	Retention	Purpose
Authentication	2 years	Security
Authorization	2 years	Security
Data access	7 years	Compliance
Admin actions	7 years	Compliance
Configuration changes	7 years	Compliance
API requests	90 days	Operations

Log Format

```
{
  "timestamp": "2024-12-24T10:30:00Z",
  "event_type": "data_access",
  "actor": {
    "id": "user-123",
    "type": "admin",
    "ip": "192.168.1.100"
  },
  "resource": {
    "type": "model",
    "id": "model-456"
  },
  "action": "read",
  "outcome": "success",
  "metadata": {}
}
```

Log Protection

- Logs are immutable (write-once)
- Logs are encrypted at rest
- Access requires special IAM role
- Log deletion requires dual approval

Incident Response

Classification

Severity	Response Time	Examples
Critical	1 hour	Data breach, service down
High	4 hours	Attempted breach, partial outage
Medium	24 hours	Policy violation
Low	72 hours	Minor security event

Breach Notification

Jurisdiction	Requirement	Timeline
GDPR	DPA + affected users	72 hours
HIPAA	HHS + affected individuals	60 days
State laws	Varies by state	Varies

Vendor Management

Approved Sub-Processors

Vendor	Purpose	Location	DPA
AWS	Infrastructure	Global	Yes
OpenAI	AI provider	US	Yes
Anthropic	AI provider	US	Yes
Google Cloud	AI provider	Global	Yes

Vendor Assessment

Annual assessment includes: - Security questionnaire - SOC 2 report review - Penetration test results - Insurance verification

Contact

Role	Contact
Data Protection Officer	dpo@radiant.example.com
Security Team	security@radiant.example.com
Compliance Team	compliance@radiant.example.com