CALMSHELL EXPANDED COMPLIANCE FRAMEWORK

Comprehensive Governance, Operations, and Implementation Guide

Canada / Ontario Edition — Version 2.0

EXECUTIVE SUMMARY

The CALMSHELL Expanded Compliance Framework provides a complete governance architecture for operating a digital mental health platform in Canada. This document extends the foundational framework with detailed operational procedures, comprehensive policy templates, implementation guidelines, and compliance monitoring systems.

Framework Status: Production-Ready
Jurisdiction: Canada / Ontario
Effective Date: January 1, 2026
Last Updated: June 2026

TABLE OF CONTENTS

---

1. ORGANIZATIONAL STRUCTURE & GOVERNANCE

1.1 Governance Hierarchy

```
Board of Directors / Founder
```

```
    ↓
Executive Director
    ├─ Clinical Governance Lead
    ├─ Privacy & Compliance Officer
    ├─ Chief Technology Officer
    ├─ Chief Financial Officer
```

```
    └─ Community & Operations Lead
```

1.2 Governance Functions & Responsibilities

Executive Governance

Responsible For:

- Strategic direction and organizational oversight
- Board-level decision making and accountability
- Funding, partnerships, and stakeholder relations
- Regulatory compliance oversight
- Annual governance review and updates

Key Functions:

- Executive meetings (monthly minimum)
- Board reporting (quarterly)
- Strategic planning (annual)
- Stakeholder engagement (ongoing)

Clinical Governance

Responsible For:

- Therapist credentialing and verification
- Clinical safety protocols and standards
- Crisis escalation procedures
- Care quality assurance
- Professional development and training

- Adherence to professional standards

Key Functions:

- Therapist onboarding and verification
- Clinical policy development
- Crisis response protocols
- Quality assurance reviews (quarterly)
- Professional development programs
- Incident investigation and response

Privacy & Compliance Governance

Responsible For:

- PHIPA compliance (Ontario health information)
- PIPEDA compliance (personal information)
- AODA compliance (accessibility)
- Consent management
- Breach notification and response
- Privacy impact assessments
- Data retention and deletion

Key Functions:

- Privacy policy development and updates
- Consent form management
- Breach investigation and notification
- Audit and compliance monitoring
- Third-party vendor management
- Privacy training and awareness

Technology Governance

Responsible For:

- Cybersecurity and infrastructure security
- Platform security and encryption
- Data backup and disaster recovery
- System uptime and reliability
- Penetration testing and vulnerability management
- Technology compliance standards

Key Functions:

- Security infrastructure management
- Incident response (technology)

- Backup and recovery procedures
- Vulnerability assessments
- Security updates and patches
- Technology audit and monitoring

Community & Operations Governance

Responsible For:

- Community standards and moderation
- Operational procedures
- User support and experience
- Institutional partnerships
- Workplace wellness programs
- Community safety and moderation

Key Functions:

- Community moderation and standards enforcement
- User support and complaint resolution
- Institutional relationship management
- Operational policy development
- Community feedback and improvement

1.3 Decision-Making Framework

Decision Type	Authority	Approval Process	Timeline
Clinical policy changes	Clinical Governance	Clinical review + Executive approval	30 days
Privacy/compliance changes	Privacy Officer	Privacy review + Executive approval	14 days
Technology infrastructure	CTO	Technical review + Executive approval	14 days
Financial commitments >$50K	CFO	Financial review + Board approval	30 days
Community policy changes	Community Lead	Community review + Executive approval	14 days
Crisis response protocols	Clinical Governance	Emergency approval	Immediate

Decision Type	Authority	Approval Process	Timeline
Data breach response	Privacy Officer	Emergency approval	Immediate
Security incidents	CTO	Emergency approval	Immediate

---

2. DETAILED POLICY FRAMEWORK

2.1 Mandatory Policies (Phase 1)

2.1.1 Terms of Service Policy

Purpose: Define the legal relationship between Calmshell and users

Key Components:

- User eligibility and account creation
- Prohibited uses and content
- Intellectual property rights
- Limitation of liability
- Dispute resolution
- Termination conditions
- Modification rights

Compliance Requirements:

- Clear, accessible language
- Specific disclaimers for mental health services
- Emergency limitation statements
- Professional responsibility disclaimers

2.1.2 Privacy Policy

Purpose: Explain how personal and health information is collected, used, and protected

Key Components:

- Information collection practices
- Use and disclosure of information
- Retention periods

- User rights and access
- Cookies and tracking
- Third-party sharing
- International data transfers
- Policy updates

Compliance Requirements:

- PIPEDA compliance
- PHIPA compliance
- Clear opt-in/opt-out mechanisms
- Specific health information handling
- Therapy note confidentiality

2.1.3 Consent Framework Policy

Purpose: Establish clear, informed consent for all services

Four-Layer Consent Structure:

Layer 1 — Platform Consent

- Acceptance of Terms of Service
- Acceptance of Privacy Policy
- Acceptance of Community Guidelines
- Acknowledgment of platform limitations

Layer 2 — Wellness Consent

- Acknowledgment of self-guided tool limitations
- Understanding of non-emergency nature
- Acceptance of wellness boundaries
- Recognition that tools are not therapy

Layer 3 — Therapy Consent

- Understanding of telehealth risks and limitations
- Confidentiality limits (emergency exceptions)
- Crisis response procedures
- Professional qualifications of therapists
- Scope of therapy services

Layer 4 — Specialized Program Consent

- Postpartum Pathway specific consent
- Research participation consent
- Advanced monitoring consent

- Institutional program consent

2.1.4 Therapist Verification Policy

Purpose: Ensure all therapists are qualified, licensed, and compliant

Verification Requirements:

- Active provincial registration verification
- Professional liability insurance confirmation
- Background check (where applicable)
- Scope of practice verification
- Continuing education requirements
- Code of conduct agreement

Verification Process:

13 Initial application and documentation submission
14 Credential verification with regulatory college
15 Background check (if applicable)
16 Insurance verification
17 Approval and onboarding
18 Annual renewal verification

Ongoing Compliance:

- Annual credential renewal
- Quarterly compliance audits
- Incident investigation
- Complaint resolution
- Continuing education tracking

2.1.5 Crisis Response Policy

Purpose: Establish procedures for identifying and responding to crisis situations

Crisis Identification:

- Suicidal ideation or intent
- Self-harm or harm to others
- Severe psychiatric symptoms
- Substance use emergencies
- Domestic violence situations

Response Procedures:

19 **Immediate Escalation:** Crisis identified → Immediate notification to therapist/platform
20 **Assessment:** Determine severity and risk level
21 **Intervention:** Provide crisis resources and support
22 **Referral:** Connect to emergency services if needed
23 **Follow-up:** Document and follow-up with user
24 **Learning:** Review and improve procedures

Crisis Resources:

- Emergency contact information (local and national)
- Crisis hotline numbers
- Emergency services (911)
- Poison control
- Mental health crisis teams
- Hospital emergency departments

2.1.6 Billing & Subscription Policy

Purpose: Establish clear billing practices and financial transparency

Billing Categories:

- Individual subscriptions (Free, Basic, Pro, Premium)
- Institutional plans (Educational, Corporate)
- Specialized programs (Postpartum Pathway)
- Therapist marketplace transactions

Key Terms:

- Subscription renewal and cancellation
- Refund policies
- Payment methods
- Billing disputes
- Institutional billing procedures
- Therapist payout procedures

2.2 Clinical Policies (Phase 1-2)

2.2.1 Scope of Practice Policy

Purpose: Define what services Calmshell provides and what it does not

In Scope:

- Wellness tools and resources
- Peer support and community
- Therapist-provided therapy (within therapist's scope)
- Mental health education
- Self-guided assessments
- Progress tracking and monitoring

Out of Scope:

- Diagnosis (unless by licensed professional)
- Emergency medical services
- Hospitalization or crisis residential care
- Medication management
- Specialized treatment (e.g., ECT)
- Court-ordered treatment

2.2.2 Telehealth Policy

Purpose: Establish standards for virtual therapy delivery

Requirements:

- Secure, encrypted video platform
- Privacy and confidentiality protections
- Technology backup procedures
- Therapist licensing in user's jurisdiction
- Informed consent for telehealth
- Emergency procedures
- Recording and documentation policies

2.2.3 Documentation Policy

Purpose: Establish standards for clinical record-keeping

Documentation Requirements:

- Therapy notes (SOAP format minimum)
- Assessment documentation
- Treatment plans
- Progress notes
- Crisis incidents
- Consent forms
- Communication records

Retention Requirements:

- Clinical records: 7 years minimum (Ontario standard)
- Consent forms: 7 years minimum
- Incident reports: 7 years minimum
- Billing records: 7 years minimum

Access & Security:

- Encrypted storage
- Role-based access control
- Audit logging
- Backup procedures

2.2.4 AI Recommendation Policy

Purpose: Establish guidelines for AI-assisted features

AI Limitations:

- Cannot diagnose
- Cannot replace clinical judgment
- Cannot provide emergency services
- Must include human oversight
- Must include clear disclaimers

AI Requirements:

- Transparency about AI use
- Human review of recommendations
- User opt-out capabilities
- Bias and fairness monitoring
- Regular auditing and testing

2.3 Community Policies (Phase 2)

2.3.1 Community Guidelines Policy

Purpose: Establish standards for respectful, safe community interaction

Prohibited Content:

- Hate speech or discrimination
- Harassment or bullying

- Violence or threats
- Sexual content or exploitation
- Clinical impersonation
- Spam or commercial promotion
- Misinformation or harmful advice

Enforcement:

- User reports and flagging
- Automated content detection
- Moderation review
- Warnings and escalation
- Suspension or removal
- Appeal process

2.3.2 Moderation Policy

Purpose: Establish procedures for community moderation and enforcement

Moderation Structure:

25 **User Reports:** Community members flag problematic content
26 **Moderation Queue:** Reports reviewed by moderation team
27 **Assessment:** Determine if content violates guidelines
28 **Action:** Warning, removal, suspension, or escalation
29 **Appeal:** User can appeal moderation decision
30 **Documentation:** All actions logged and reviewed

Escalation Procedures:

- Clinical concerns → Clinical Governance
- Legal concerns → Legal/Compliance
- Safety concerns → Crisis Response
- Institutional concerns → Institutional Lead

2.3.3 Peer Support Disclaimer Policy

Purpose: Clarify the limitations and nature of peer support

Key Disclaimers:

- Peer support is not therapy
- Peer supporters are not clinicians
- Peer support should not replace professional care
- Crisis situations require professional intervention
- Confidentiality limitations in peer support

- Peer supporters' responsibility to escalate concerns

2.4 Institutional Policies (Phase 2)

2.4.1 Institutional Data Access Policy

Purpose: Define what data institutions can access and how

Educational Institutions:

- Access to: Aggregate wellness trends, anonymized reporting, usage analytics
- Cannot access: Therapy notes, private conversations, identifiable information

Corporate Programs:

- Access to: Aggregate wellness trends, anonymized reporting, program participation
- Cannot access: Individual therapy information, health records, identifiable data

Data Aggregation Standards:

- Minimum 5 individuals per data point (to prevent re-identification)
- No identifiable information
- Aggregate reporting only
- Quarterly reporting maximum

2.4.2 Workplace Wellness Policy

Purpose: Establish standards for corporate wellness programs

Program Components:

- Wellness resources and tools
- Educational content
- Aggregate wellness reporting
- Employee assistance program (EAP) integration
- Privacy protections for employees

Employer Responsibilities:

- Confidentiality of employee health information
- Non-discrimination based on wellness data
- Clear communication of privacy protections
- Compliance with employment standards

3. CLINICAL GOVERNANCE & SAFETY

3.1 Therapist Credentialing Process

Step 1: Application

- Complete application form
- Provide credentials and documentation
- Submit professional liability insurance proof
- Agree to Calmshell standards and code of conduct

Step 2: Verification

- Verify provincial registration with regulatory college
- Confirm insurance coverage
- Conduct background check (if applicable)
- Review scope of practice

Step 3: Approval

- Clinical Governance review and approval
- Onboarding and training
- Platform access setup
- Initial supervision schedule

Step 4: Ongoing Compliance

- Annual credential renewal
- Quarterly compliance audits
- Incident investigation
- Continuing education tracking
- Annual performance review

3.2 Clinical Supervision Framework

Supervision Requirements:

- New therapists: Weekly supervision (first 3 months)
- Established therapists: Bi-weekly supervision (ongoing)
- Complex cases: Additional supervision as needed
- Crisis cases: Immediate supervision

Supervision Content:

- Case review and clinical decision-making

- Adherence to standards and policies
- Ethical issues and dilemmas
- Professional development
- Compliance and documentation

Supervision Documentation:

- Supervision notes
- Issues identified and addressed
- Action plans
- Therapist development goals
- Compliance status

3.3 Crisis Response Procedures

Crisis Identification:

- Suicidal ideation or intent
- Self-harm or harm to others
- Severe psychiatric decompensation
- Substance use emergencies
- Domestic violence
- Child abuse or neglect

Response Protocol:

Crisis Type	Immediate Action	Follow-up	Documentation
Suicidal ideation	Assess risk, provide crisis resources, contact emergency services if imminent	24-hour follow-up	Crisis incident report
Self-harm	Assess risk, provide support, refer to emergency if needed	24-hour follow-up	Crisis incident report
Harm to others	Assess risk, contact police if imminent threat	Immediate escalation	Crisis incident report
Substance emergency	Provide crisis resources, contact emergency services	24-hour follow-up	Crisis incident report
Domestic violence	Provide safety resources, refer to DV services	24-hour follow-up	Crisis incident report
Child abuse	Mandatory reporting to CAS	Immediate reporting	Incident report

Crisis Resources to Provide:

- National Suicide Prevention Lifeline: 1-833-456-4566
- Crisis Text Line: Text HOME to 741741
- Local emergency services: 911
- Local crisis teams and mental health services
- Hospital emergency departments
- Poison control: 1-800-268-9017

3.4 Quality Assurance Framework

Ongoing Monitoring:

- Case file audits (quarterly)
- Therapist performance reviews (annual)
- User satisfaction surveys
- Complaint and incident tracking
- Compliance audits

Quality Metrics:

- User satisfaction scores
- Therapist retention rates
- Complaint rates
- Crisis response times
- Documentation compliance
- Credential compliance

Improvement Process:

31 Identify quality issues through monitoring
32 Investigate root causes
33 Develop improvement plan
34 Implement changes
35 Monitor effectiveness
36 Document and communicate

---

4. PRIVACY & DATA PROTECTION

4.1 Privacy by Design Framework

Core Principles:

- Minimize data collection (collect only necessary information)

- Secure storage (encrypt all sensitive data)
- Limited access (role-based access control)
- Transparency (clear privacy policies)
- User control (data access and deletion rights)
- Accountability (audit trails and monitoring)

4.2 Data Classification & Handling

Data Type	Classification	Retention	Access	Protection
Personal (name, email)	Sensitive	User request or 3 years	Limited	Encrypted
Health information	Highly sensitive	7 years	Restricted	Encrypted + audit log
Therapy notes	Highly sensitive	7 years	Therapist + user	Encrypted + audit log
Billing information	Sensitive	7 years	Finance only	Encrypted
Aggregate analytics	Non-sensitive	Indefinite	Authorized staff	Standard security

4.3 Consent Management

Consent Types:

- Platform consent (Terms of Service)
- Privacy consent (data collection and use)
- Therapy consent (clinical services)
- Specialized program consent (postpartum, research)

Consent Documentation:

- Consent forms with timestamps
- Version control of consent forms
- User acknowledgment records
- Withdrawal of consent procedures

Consent Withdrawal:

- Users can withdraw consent at any time
- Withdrawal procedure clearly documented
- Data handling after withdrawal specified
- User notified of implications

4.4 Data Subject Rights

User Rights:

- Right to access personal information
- Right to correct inaccurate information
- Right to delete information (subject to legal retention)
- Right to data portability
- Right to withdraw consent
- Right to lodge complaints

Access Request Process:

37 User submits access request
38 Verify user identity
39 Locate and compile information
40 Provide information within 30 days
41 Document request and response

4.5 Data Breach Response

Breach Detection:

- Unauthorized access
- Data theft or loss
- Accidental disclosure
- System compromise

Response Protocol:

42 **Immediate:** Contain breach, assess scope, notify leadership
43 **Investigation:** Determine what data was accessed, how, when
44 **Notification:** Notify affected individuals within 30 days (if high risk)
45 **Reporting:** Report to Privacy Commissioner if required
46 **Remediation:** Implement fixes to prevent recurrence
47 **Documentation:** Document all actions and findings

Notification Requirements:

- Notify individuals if personal health information exposed
- Notify Privacy Commissioner if breach affects >500 individuals
- Notify regulatory bodies if required
- Maintain breach notification log

---

5. TECHNOLOGY & SECURITY

5.1 Security Infrastructure

Authentication:

- Bcrypt password hashing
- Multi-factor authentication (MFA) for sensitive accounts
- JWT session tokens
- Role-based access control (RBAC)
- Session timeouts

Encryption:

- HTTPS for all communications
- AES-256 encryption for data at rest
- TLS 1.2+ for data in transit
- Encrypted backups
- Key management procedures

Infrastructure:

- Secure cloud hosting (AWS, Azure, or equivalent)
- Firewalls and intrusion detection
- DDoS protection
- Regular security patches
- Backup and disaster recovery

5.2 Vulnerability Management

Vulnerability Assessment:

- Annual penetration testing
- Quarterly vulnerability scans
- Code review and testing
- Dependency scanning
- Security audits

Incident Response:

- Vulnerability discovered → Assessment
- Risk determination → Prioritization
- Patch development → Testing
- Deployment → Verification
- Documentation → Learning

5.3 Monitoring & Logging

Audit Logging:

- User authentication and access
- Data access and modifications
- Administrative actions
- System errors and warnings
- Security events

Log Retention:

- Audit logs: 1 year minimum
- Security logs: 2 years minimum
- Backup logs: 1 year minimum
- Compliance logs: 7 years minimum

Monitoring Procedures:

- Real-time alert monitoring
- Suspicious activity detection
- Regular log review
- Incident investigation
- Trend analysis

---

6. COMMUNITY & INSTITUTIONAL GOVERNANCE

6.1 Community Moderation Framework

Moderation Team Structure:

- Moderation Lead
- Community Moderators
- Escalation specialists
- Clinical consultants

Moderation Workflow:

48 User reports content or automated detection
49 Moderator reviews content
50 Determine if violation occurred
51 Take action (warning, removal, suspension)
52 Document action
53 User can appeal

Actions Available:

- Warning (first offense)
- Content removal (policy violation)
- Temporary suspension (repeated violations)
- Permanent removal (severe violations)
- Escalation to clinical team (safety concerns)

6.2 Institutional Partnerships

Educational Institutions:

- Counselor dashboards
- Wellness analytics
- Student support resources
- Privacy protections
- Data access limitations

Corporate Programs:

- Employee wellness resources
- Aggregate reporting
- EAP integration
- Privacy protections
- Compliance with employment standards

Healthcare Institutions:

- Therapist referral pathways
- Continuity of care
- Clinical coordination
- Data sharing agreements
- Compliance with healthcare standards

---

7. FINANCIAL & BILLING COMPLIANCE

7.1 Billing Structure

Plan	Price	Features	Audience
Free	$0	Basic wellness tools	Individual users
Basic	$9.99/mo	Wellness + community	Individual users
Pro	$19.99/mo	Wellness + therapy (limited)	Individual users
Premium	$49.99/mo	Unlimited therapy + all features	Individual users
Institutional	Custom	Custom features + reporting	Educational/Corporate
Postpartum Pathway	$99/month	Specialized postpartum support	Postpartum individuals

7.2 Payment Processing

Stripe Integration:

- Secure payment processing
- Subscription management
- Refund handling
- Payout management
- PCI compliance

Payment Flow:

- User selects plan
- Stripe payment processing
- Subscription activation
- Recurring billing
- Refund/cancellation handling

7.3 Refund Policy

Refund Eligibility:

- Full refund within 7 days of purchase
- Prorated refund for cancellation mid-month

- No refund for used services beyond 7 days
- Institutional plans: Custom refund terms

Refund Process:

54 User requests refund
55 Verify eligibility
56 Process refund through Stripe
57 Notify user of refund status
58 Document refund

7.4 Financial Reporting

Required Reports:

- Monthly revenue and usage
- Subscription metrics
- Churn and retention rates
- Institutional billing
- Therapist payouts
- Annual financial audit

---

8. RESEARCH & ASSESSMENT GOVERNANCE

8.1 Assessment Standards

Assessment Requirements:

- Clear disclaimers (not diagnostic)
- Evidence-based instruments
- Validated scoring
- Interpretation guidelines
- Professional review option
- Results documentation

Assessment Types:

- Mental health screening (PHQ-9, GAD-7)
- Wellness assessments
- Progress tracking
- Outcome measurement

8.2 Research Governance

Research Activities:

- Randomized controlled trials
- Observational studies
- Outcome research
- Academic partnerships

Research Requirements:

- Ethics review (REB approval if required)
- Informed consent
- Data separation and security
- Publication standards
- Funder transparency

Research Consent:

- Separate consent form
- Clear explanation of research
- Voluntary participation
- Right to withdraw
- Data use and publication

---

9. RISK MANAGEMENT & INCIDENT RESPONSE

9.1 Risk Categories & Mitigation

Risk Category	Potential Risks	Mitigation Strategies	Monitoring
Clinical	Unsafe advice, crisis mishandling, scope violations	Therapist verification, supervision, crisis protocols	Case audits, complaints
Technology	Outages, breaches, data loss	Infrastructure redundancy, security, backups	System monitoring, audits
Legal	Regulatory non-compliance, liability	Policies, compliance monitoring, legal review	Compliance audits
Reputational	Unsafe moderation, misinformation	Community standards, moderation, fact-checking	Social listening, feedback

Risk Category	Potential Risks	Mitigation Strategies	Monitoring
Financial	Billing errors, fraud, payment issues	Stripe integration, auditing, controls	Financial audits

9.2 Incident Response Framework

Incident Types:

- Clinical incidents (crisis, unsafe advice)
- Technology incidents (outages, breaches)
- Security incidents (unauthorized access)
- Compliance incidents (policy violations)
- Reputational incidents (misinformation, complaints)

Response Protocol:

59 **Detection:** Incident identified through monitoring or reporting
60 **Assessment:** Determine severity and impact
61 **Escalation:** Notify appropriate leadership
62 **Containment:** Prevent further harm or spread
63 **Investigation:** Determine root cause
64 **Remediation:** Fix underlying issues
65 **Communication:** Notify affected parties
66 **Documentation:** Record all actions
67 **Learning:** Implement improvements

Incident Documentation:

- Incident type and severity
- Timeline of events
- Root cause analysis
- Actions taken
- Outcomes and impact
- Lessons learned
- Preventive measures

---

10. IMPLEMENTATION ROADMAP

Phase 1: Foundation (Months 1-3)

Deliverables:

- Terms of Service
- Privacy Policy
- Consent Framework
- Therapist Verification Process
- Billing Policies
- Crisis Response Procedures
- Initial governance structure

Success Metrics:

- All policies documented and approved
- Therapist verification process operational
- Crisis response procedures tested
- Governance meetings established

Phase 2: Operational (Months 4-6)

Deliverables:

- AI Governance framework
- Institutional Governance policies
- Community Moderation system
- Security Monitoring system
- Clinical Supervision framework
- Quality Assurance procedures

Success Metrics:

- Moderation system operational
- Security monitoring active
- Clinical supervision schedule established
- Quality metrics baseline established

Phase 3: Advanced (Months 7-12)

Deliverables:

- Research Governance framework
- Specialized Pathways (Postpartum)
- Advanced Analytics
- Compliance Audit procedures

- Continuous improvement system
- National scaling preparation

Success Metrics:

- Research protocols established
- Specialized pathways operational
- Compliance audit completed
- Scaling roadmap developed

---

11. COMPLIANCE MONITORING & AUDIT

11.1 Compliance Monitoring Schedule

Area	Frequency	Responsibility	Documentation
Therapist credentials	Annual	Clinical Governance	Credential verification log
Clinical supervision	Ongoing	Clinical Governance	Supervision records
Crisis response	Per incident	Clinical Governance	Incident reports
Privacy compliance	Quarterly	Privacy Officer	Compliance audit report
Security monitoring	Continuous	CTO	Security logs and alerts
Community moderation	Ongoing	Community Lead	Moderation reports
Billing accuracy	Monthly	CFO	Billing audit report
Policy compliance	Quarterly	Compliance Officer	Compliance checklist

11.2 Annual Compliance Audit

Audit Scope:

- Policy compliance

- Regulatory alignment
- Data protection
- Security controls
- Clinical standards
- Community standards
- Financial controls

Audit Process:

68 Audit planning and scope definition
69 Data collection and review
70 Testing and verification
71 Findings documentation
72 Recommendations development
73 Management response
74 Remediation tracking
75 Audit report finalization

Audit Report Contents:

- Executive summary
- Findings by area
- Risk assessment
- Recommendations
- Management responses
- Timeline for remediation

---

12. APPENDICES & TEMPLATES

Appendix A: Policy Templates

Template 1: Terms of Service

- User eligibility
- Prohibited uses
- Intellectual property
- Liability limitations
- Dispute resolution
- Termination conditions

Template 2: Privacy Policy

- Information collection
- Use and disclosure
- Retention periods
- User rights
- Cookies and tracking
- Third-party sharing

Template 3: Consent Forms

- Platform consent
- Privacy consent
- Therapy consent
- Specialized program consent

Template 4: Therapist Agreement

- Scope of practice
- Professional standards
- Supervision requirements
- Code of conduct
- Compliance obligations

Appendix B: Governance Procedures

Procedure 1: Therapist Credentialing

- Application process
- Verification procedures
- Approval process
- Onboarding procedures
- Annual renewal

Procedure 2: Crisis Response

- Identification procedures
- Assessment procedures
- Intervention procedures
- Referral procedures
- Documentation procedures

Procedure 3: Data Breach Response

- Detection procedures
- Investigation procedures
- Notification procedures
- Remediation procedures

- Documentation procedures

Procedure 4: Complaint Resolution

- Complaint intake
- Investigation
- Resolution
- Appeal process
- Documentation

Appendix C: Compliance Checklists

Checklist 1: Monthly Compliance

- ☐Therapist credential verification
- ☐Crisis response procedures reviewed
- ☐Community moderation reviewed
- ☐Billing accuracy verified
- ☐Security monitoring reviewed

Checklist 2: Quarterly Compliance

- ☐Privacy compliance audit
- ☐Clinical supervision review
- ☐Quality assurance metrics
- ☐Policy compliance review
- ☐Incident review and learning

Checklist 3: Annual Compliance

- ☐Full compliance audit
- ☐Regulatory alignment review
- ☐Policy updates and approvals
- ☐Governance structure review
- ☐Strategic planning and updates

CONCLUSION

The CALMSHELL Expanded Compliance Framework provides a comprehensive governance architecture for operating a digital mental health platform in Canada. This framework ensures:

✅ **User Safety** – Through clinical governance, crisis procedures, and quality assurance
✅ **Privacy Protection** – Through PHIPA/PIPEDA compliance and data protection
✅ **Regulatory Alignment** – Through comprehensive policy and procedure compliance
✅ **Operational Excellence** – Through clear governance, monitoring, and continuous improvement
✅ **Institutional Trust** – Through transparency, accountability, and professional standards

Implementation Status: Ready for immediate deployment
Next Steps: Begin Phase 1 implementation with policy finalization and governance structure establishment

---

REFERENCES

76 Personal Information Protection and Electronic Documents Act (PIPEDA)
77 Personal Health Information Protection Act (PHIPA)
78 Accessibility for Ontarians with Disabilities Act (AODA)
79 Ontario Colleges of Health Professions
80 Canadian Standards Association (CSA) - Digital Trust & Privacy
81 MHCC - Mental Health Commission of Canada

Document Version: 2.0
Last Updated: June 2026
Status: Production-Ready
Jurisdiction: Canada / Ontario
Classification: Confidential - Internal Use