Risk Assessment - MindMend

Threat Landscape

MindMend operates within a threat landscape defined by its fully virtual, cloud-native architecture. As a digital health provider, its proprietary SaaS platform integrates AI and data analytics capabilities, processing and storing Personal Health Information (PHI) and Personally Identifiable Information (PII), making it an attractive target for cyber threats.

External

- Cyber criminal groups interested in Personal Health Information (PHI):
    - Ransomware & Malware: A healthcare platform storing sensitive PHI is a lucrative target for ransomware gangs seeking high payouts to unlock patient or operational data.
    - State-sponsored actors targeting innovative AI-driven medical technologies for economic or strategic advantage
- Phishing and Social Engineering: Employees are more susceptible to phishing attacks when a fully remote team is involved.
- Exfiltration of Intellectual Property by competitors:
    - AI databases
    - AI Models
    - Matching algorithms
    - Analytics tools
- API Exploitation: AI-powered therapy matching and telehealth are likely to expose API's linked to data extraction or service disruption.
- DDoS Attacks: Competitors or Hacktivist groups might try to disrupt services to push customers to their platform.

Internal

- Source code repositories: Poorly secured GitHub repositories
- Cloud Misconfigurations: Unsecured S3 buckets, overprivileged IAM roles and poorly designed WAF rules
- Endpoint Compromise: Insecure BYOD configurations, insecure home WiFi configurations and watering hole attacks.
- Collaboration Tool Compromise: Slack, Google Drive and Confluence can become compromised.
- Network Traffic: Lack of outbound filtering and traffic monitoring can allow data exfiltration via HTTP or DNS Tunnelling.
- Third Party Risk: Integration with analytics and compliance vendors could introduce vulnerabilities if not held to high security standards.

Emerging Threats

- AI Manipulation: AI Prompt injection can subvert customer outputs or exfiltrate customer data.

- Deepfakes and Identity fraud: Cloning voices and creating fake videos to impersonate customers

Key Risk Areas

Client Risks

1. Patients becoming reliant on or misinterpreting AI-generated therapy recommendations.
2. Inaccurate or incomplete patient disclosures may lead to suboptimal AI recommendations, posing clinical and reputational risks.
3. Service availability in emergency situations could cause medical problems with customers and tarnish MindMend
4. Misuse of platform features or misunderstanding of AI outputs without proper disclaimers and clinician oversight

Contractual Obligations

1. Failure to meet ISO 27001 milestones could affect customer contracts
2. Discrepancies with data flow in relation to medical laws in different jurisdictions
3. Inaccurate AI-driven therapy matching could be construed as a failure to deliver contracted service levels, affecting liability and trust

Data Risks

1. Exfiltration of proprietary AI models, training data, and business logic
2. Unauthorised access or leakage of PHI, in violation of the Privacy Act 1988
3. Exposure of stored or transmitted payment data, violating PCI DSS requirements

Software Risks

1. Insufficient security controls in CI/CD pipelines or container orchestration (e.g., Kubernetes misconfigurations)
2. Vulnerabilities in the AI model could leak data
3. Insecure and unpatched database servers
4. Risk of third-party libraries or open-source component vulnerabilities (GitHub repositories)

Vendor Risks

1. Vendors with low security policies could expose MindMend's shared data
2. Dependence on a single vendor could disrupt the platform if the vendor becomes compromised in any way
3. Insecure vendor APIs could expose MindMend’s data
4. Inadequate third-party due diligence or ongoing vendor monitoring can introduce persistent vulnerabilities into the environment

Staff Risks

1. Lack of security training will result in a lack of security awareness
2. Lack of proper onboarding of staff could result in platform exposure

3. Overprivileged user accounts or insufficient access revocation post-employment increase insider threat potential
4. Shadow IT by remote staff using unauthorised tools or services

Operational Risks

1. Poor security posture could result in inadequate incident response
2. Insufficient system and control documentation impedes audits, onboarding, and incident investigation.
3. Lack of formal business continuity and disaster recovery planning for cloud-based architecture

Control Gaps

Risk Register

Tier	Risk	Desc	Owner	Likelihood	Impact	Treatment
Client Risks				3	4	12
	1	Patients becoming reliant on or misinterpreting AI-generated therapy recommendations.	Dr. Nina Hayes	3	4	Mitigate
	2	Inaccurate or incomplete patient disclosures may lead to suboptimal AI recommendations, posing clinical and reputational risks.	Olivia Mercer Dr. Nina Hayes	4	3	Mitigate
	3	Service availability in emergency situations could cause medical problems with customers and tarnish MindMend	Priya Desai Daniel Kim	2	5	Mitigate
	4	Misuse of platform features or misunderstanding of AI outputs without proper disclaimers and clinician oversight	Olivia Mercer	3	4	Mitigate
Contractual Obligations				2.66	4	10.4
	1	Failure to meet ISO 27001 milestones could affect customer contracts	Olivia Mercer	3	4	Mitigate
	2	Discrepancies with data flow in relation to medical laws in different jurisdictions	Olivia Mercer	3	4	Monitor
	3	Inaccurate AI-driven therapy matching could be construed as a failure to deliver contracted service levels, affecting liability and trust	Dr. Nina Hayes/Olivia Mercer	2	4	Mitigate
Data Risks				3.33	4.33	14.3
	1	Exfiltration of proprietary AI models, training data, and business logic	Priya Desai	3	4	Mitigate
	2	Unauthorised access or leakage of PHI, in violation of the Privacy Act 1988	Priya Desai	4	5	Mitigate
	3	Exposure of stored or transmitted payment data, violating PCI DSS requirements	Priya Desai	3	4	Mitigate
Software Risks				3	3.75	11.25
	1	Insufficient security controls in CI/CD pipelines or container orchestration (e.g., Kubernetes misconfigurations)	Priya Desai	3	4	Mitigate
	2	Vulnerabilities in the AI model could leak data	Priya Desai	3	4	Mitigate
	3	Insecure and unpatched database servers	Priya Desai	2	4	Mitigate
	4	Risk of third-party libraries or open-source component vulnerabilities (GitHub repositories)	Priya Desai	4	3	Mitigate

Vendor Risks				3.5	3.75	13.12
	1	Vendors with low security policies could expose MindMend's shared data	Priya Desai	3	4	Mitigate
	2	Dependence on a single vendor could disrupt the platform if the vendor becomes compromised in any way	Daniel Kim	4	4	Mitigate
	3	Insecure vendor APIs could expose MindMend's data	Priya Desai	3	4	Mitigate
	4	Inadequate third-party due diligence or ongoing vendor monitoring can introduce persistent vulnerabilities into the environment	Olivia Mercer	4	3	Mitigate
Staff Risks				3.5	3.5	12.25
	1	Lack of security training will result in a lack of security awareness	Laura Simmons	4	4	Mitigate
	2	Lack of proper onboarding of staff could result in platform exposure	Laura Simmons	3	3	Mitigate
	3	Overprivileged user accounts or insufficient access revocation post-employment increase insider threat potential	Laura Simmons	3	4	Mitigate
	4	Shadow IT by remote staff using unauthorised tools or services	Laura Simmons	4	3	Mitigate
Operational Risks				3.33	4.33	14.41
	1	Poor security posture could result in inadequate incident response	Daniel Kim	3	5	Mitigate
	2	Insufficient system and control documentation impedes audits, onboarding, and incident investigation.	Daniel Kim	4	3	Mitigate
	3	Lack of formal business continuity and disaster recovery planning for cloud-based architecture	Daniel Kim	3	5	Mitigate

Risk = Medium