Privacy Operations Center

Bringing privacy initiatives together.

headspace
Context

headspace + headspace care

Wellness Healthcare

Used in 190 countries around the world
Over 100 million covered lives
More than 4,000 clients and partners
Why?

- Legal and regulatory requirements
  - compliance with GDPR, CCPA, HIPAA.

- Mandatory requirements from app stores
  - Apple’s deletion request.

- Prevent financial and reputational loss
  - 434 breaches reported to HHS as of Aug 30, 2023.

- Ongoing media scrutiny
  - Mozilla’s ‘Privacy Not Included’ report.
But most importantly...

Privacy is an existential risk.
What constitutes a POC?
Data Management v/s Data Governance

Organize

Store

Classification

Protect

Maintain

Frameworks

Policies

Strategic

Procedures

Stewardship
# Headspace Data Classification

<table>
<thead>
<tr>
<th>Parent Classification</th>
<th>Child Classification (US / International)</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitive</td>
<td>PHI / Health</td>
<td>Health records, chat transcripts</td>
</tr>
<tr>
<td></td>
<td>Sensitive Personal Information / Special Category Data</td>
<td>Government ID, religious beliefs</td>
</tr>
<tr>
<td>Private</td>
<td>PII / Personal Data</td>
<td>Name, Email (not direct identifiers to PHI)</td>
</tr>
<tr>
<td>Customer Confidential</td>
<td>Customer Confidential</td>
<td>Eligibility files</td>
</tr>
<tr>
<td>Company Confidential</td>
<td>Company Confidential / Internal</td>
<td>Business plans, meditations</td>
</tr>
<tr>
<td>Research</td>
<td>Research</td>
<td>De-identified PHI, anonymized aggregate data sets</td>
</tr>
<tr>
<td>Public</td>
<td>Public</td>
<td>Marketing materials, press releases</td>
</tr>
</tbody>
</table>
Privacy & Security Review Process

Product

Start → Drafts the PRD → PRD → Submits the Risk Review JIRA Form → Approved

Engineering

Product

Drafts the Tech Spec → Tech Spec

Legal, Privacy, Security

Risk Review Plan

Schedule Meeting with key stakeholders → Legal Review → Privacy Review → Threat Modeling

Follow up with Eng/Product Team? → Yes → Summarize Recommendations → Product Risk Review Request → Perfect report with remediation proposal

No → Perfect

Yes → Schedule Perfect

Perfect
Shifting Privacy Left & Right

Embed privacy tools as part of SDLC

Automated Data Classification & Labeling

Data Governance
Privacy Awareness

- Headspace specific HIPAA training
- Monthly office hours
- Dedicated Slack channels to discuss privacy issues
- Privacy Intranet & feedback form
- Master Privacy FAQ
Key Lessons

Security **enables** Privacy.

#putmembersfirst

Building world’s most trusted mental healthcare organization.
Resources

- CRISC Exam Handbook, Chapter 17, Information Security & Privacy Principles - [Link](#)
- Privacy conferences
  - PEPR - https://www.usenix.org/conference/pepr23
  - Rise of Privacy Tech - https://www.riseofprivacytech.com/
- A Taxonomy of Privacy - [Link](#)
- IAPP - [iapp.org](http://iapp.org)
Team

- Alex Boisvert, SVP Engineering
- Puneet Thapliyal, CISO
- Ken Stineman, CPO
- Garth Davis, Privacy Counsel
- Jamie Firth, Legal Counsel
- Robert Khirallah, Infra & AppSec Manager
- Brendan Sweeney, Staff Cloud Security Engineer
- Michael Blake, Sr AppSec Engineer