Privacy Operations Center

Bringing privacy initiatives together.

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 <u>existential risk</u>.

What constitutes a POC?

Governance & Management

Security & Awareness

Privacy Operations Center

Partnerships

Tools
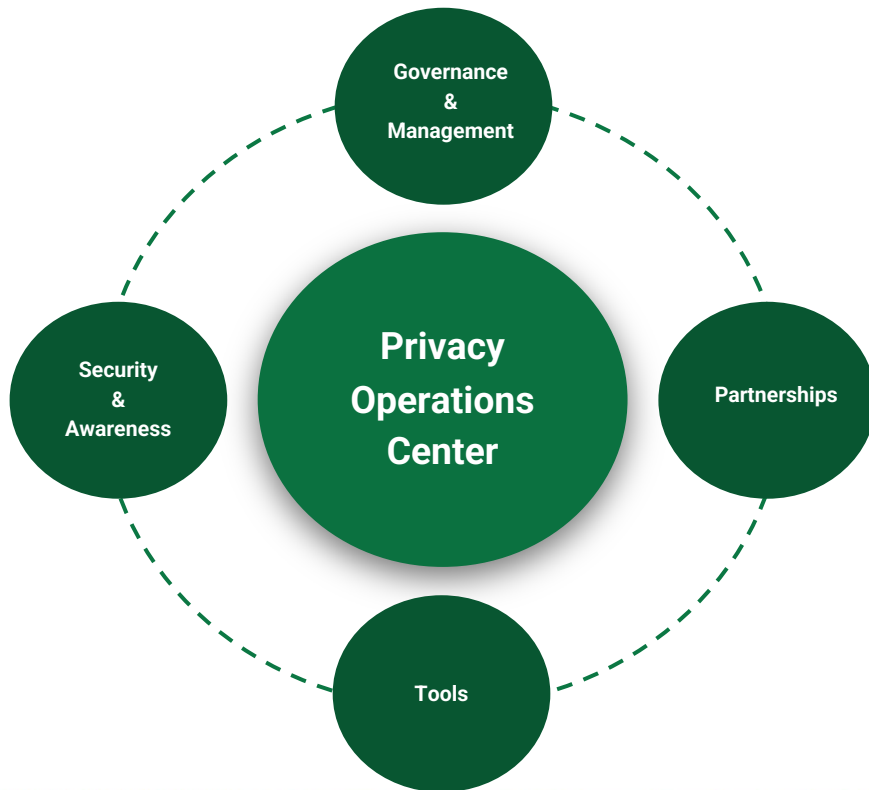
Data Management v/s Data Governance

Organize

Frameworks

Store

Policies

Classification

Strategic

Protect

Procedures

Maintain

Stewardship

Headspace Data Classification

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

Privacy & Security Review Process

Product

Engineering

**Legal,
Privacy,
Security**

Product Risk Review Process
Shobhit Mehta | August 30, 2023
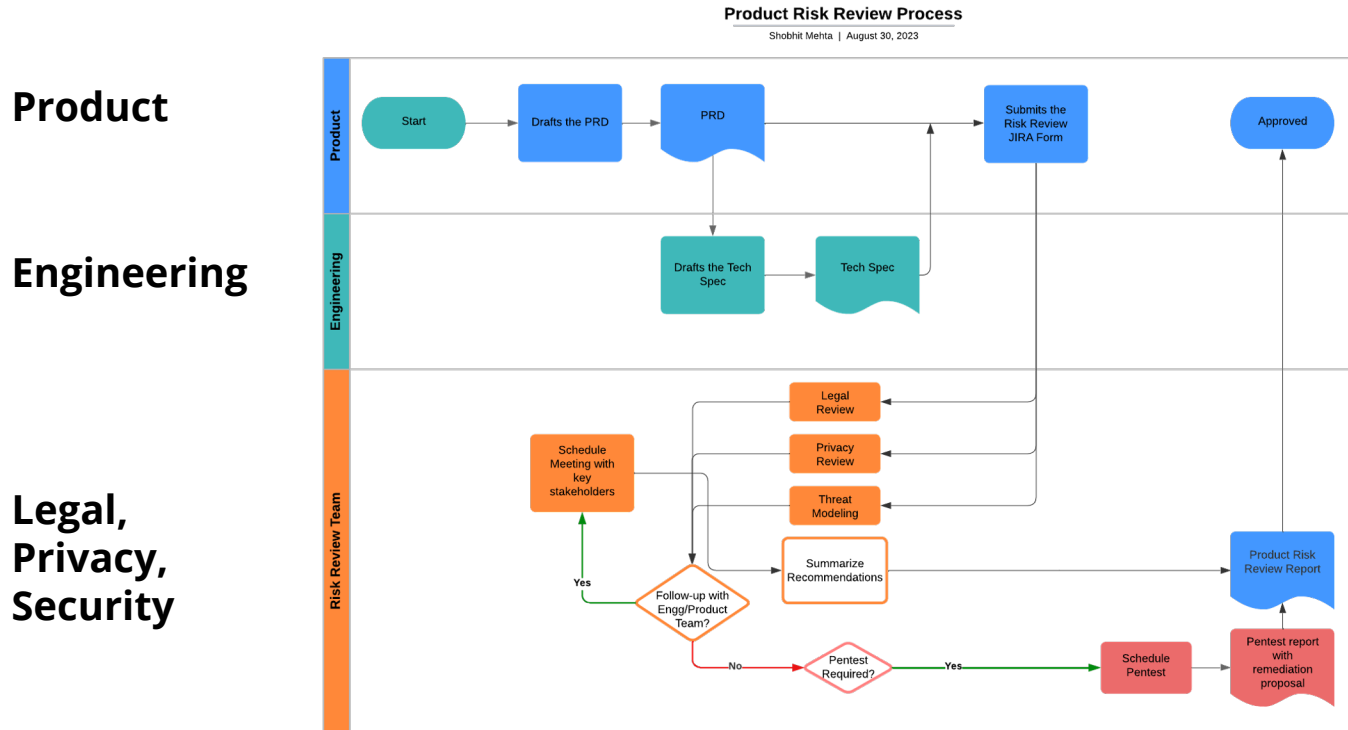
Shifting Privacy Left & Right

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](#)

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