Health care privacy on the ground:

Key challenges and practical solutions

By Elimu Kajunju, Former privacy leader, Google and
Michael Hamilton, Senior director of privacy, Adobe

Contents

Health care privacy on the ground:

Key challenges and practical solutions

By Elimu Kajunju, Former privacy leader, Google and
Michael Hamilton, Senior director of privacy, Adobe

The views, thoughts and opinions expressed in this white paper belong solely to the authors and do not reflect the official policy or position of their respective organizations or any other organization with which the authors are affiliated.

Health care privacy sits at the center of a deep tension. On one hand, there is a strong push by health care and technology companies to use and leverage ever-increasing amounts of health information for a variety of purposes, including precision medicine.[1] On the other hand, regulators around the world treat health information as sensitive data, restricting and limiting its uses. The navigation of this tension is at the core of a health care privacy professional's job.

The goal of this paper is to tackle some of the most pressing challenges in-house health care privacy teams face and describe concrete solutions. We interviewed more than 20 in-house privacy experts for on-the-ground insights and ideas. The interviewees were primarily from the health care industry, but we also interviewed those working on privacy outside of health care. The challenges faced by nonhealth care privacy teams, it turns out, have a great deal of overlap with the challenges faced by health care privacy teams. To supplement the insights from privacy experts, we also interviewed other roles that work closely with privacy, including product counsel, general counsel and chief information security officers.[2]

This white paper supplements and builds upon a previous IAPP white paper from October 2021: "Privacy as a competitive differentiator – Building an effective and strategic health care privacy program."

[1] "Health information" is used throughout the document to generally mean personally identifiable health information related to the physical or mental health of a natural person, including the provision of health care services that reveal information about their health status.

[2] We thank all contributors to this article, including the following individuals: Joe Askhouti, Patrick Curry, Lothar Determann, Mitchell Granberg, Dan Guggenheim, Stefanie Head, Jesse Hwang, Ravi Inthiran, Sheila Jambekar, Faith Knight Myers, Deven McGraw, Veronica Sander and Aaron Weller.

Role of the health care privacy team

This section describes the work performed by a health care privacy team and options for the privacy team's reporting structure.

Scope of work

The primary role of a company's health care privacy team is to ensure its operations regarding health information comply with the legal and contractual requirements that apply to the information. The privacy team's job is to know the rules that apply to the business and develop policies, processes, procedures, checklists, practices, tools and trainings to help the company satisfy its obligations and achieve its data strategy goals. A company's privacy team is often also the face of privacy for its customers, vendors, business partners, patients and regulators. Below is a brief description of the seven core pillars of work performed by a health care privacy team. For more details on these pillars, see the IAPP white paper referenced above.

Legal analysis

Legal analysis is the work of analyzing laws, regulations, regulatory guidance and other resources to understand how they apply to the company. Privacy teams within companies are particularly focused on applying privacy laws to the particular facts of the company and making decisions about how to comply with sometimes ambiguous privacy requirements.

Policies, procedures and guidelines

Policies, procedures and guidelines are mechanisms a privacy team leverages to implement privacy compliance within a company. These are the privacy rules the company will follow. More than mere recitations of the law, these rules should reflect a practical and reasoned application of the law to the company. They should be simple enough that those with limited privacy knowledge are able to use and apply them in their jobs.

Contracting

Privacy involves a significant amount of transactional work. Privacy laws often require very specific contract language. Many customers also impose strict requirements around privacy and health information use beyond the law. Accordingly, privacy teams may spend a significant amount of time negotiating privacy terms with customers, vendors and business partners. Privacy teams often negotiate business associate agreements under the Health Insurance Portability and Accountability Act, data processing agreements, standard contractual clauses and security exhibits, working closely with the security team. When the privacy team is not directly negotiating these types of agreements, it may develop playbooks for other teams, such as commercial or procurement legal, to leverage. Playbooks typically cover the standard negotiating points and fallbacks, directing teams to engage with the privacy team on complex or novel privacy questions.

Product counseling

The privacy team counsels the company on privacy issues related to the products and services it delivers. The privacy team may leverage product counsel or business-unit counsel for privacy counseling. It is, therefore, critical for the product or business-unit counsel to have sufficient privacy expertise to, at a minimum, flag privacy issues. Often privacy teams provide privacy-by-design tools, such as playbooks and checklists, to assist in the issue-spotting or design processes. Product counseling also involves reviewing vendors who provide products or features to the company.

Privacy operations

Privacy operations is a broad bucket of activities that comprise the operational aspects of a privacy program. Most of the privacy work that is not part of any of the other pillars falls under this category. It may include training, communications such as privacy newsletters, incident management, complaints, individual privacy rights requests and privacy notices. Many companies use privacy program management tools to help manage privacy operations functions.

Privacy risk assessments

Privacy risk assessments include the continuing work to evaluate privacy risks within the company and ensure they are appropriately documented and addressed. It includes periodic self-assessments performed by members of the privacy team, or an adjacent team like compliance, and assessments performed by independent parties such as an internal audit function or third-party auditor.

Security

Security forms an integral part of a privacy program. While privacy teams are not generally directly responsible for implementing security requirements, they are responsible for ensuring security obligations related to personal information, both under the law and pursuant to contracts, are implemented by the organization. Privacy teams sometimes oversee and usually support the work carried out by the security team. This is largely because many privacy controls rely on security controls being in place. For example, privacy controls may require that only nurses have access to patient information. To implement this control, the system needs to be configured so only individuals identified as nurses can access screens containing patient information. If it is inappropriately configured, i.e., the security controls have not been designed appropriately, someone who is not a nurse may be able to access patient information.

Reporting structure

The next key question regards where a privacy team should sit within an organization. Should privacy be a legal function reporting directly to the general counsel or should it be treated as a compliance function reporting to the chief compliance officer? What other options are there?

Compliance

One view is that privacy teams should report into compliance. Under this approach, one part of the organization needs to define what the law or regulation is, what parts of the company need to meet those requirements, and what the company policy should be based on that law or regulation. That is legal analysis and legal advice.

The compliance part of the organization then builds a program around that legal analysis and advice. The program should address the business's procedures, necessary controls, training of personnel, monitoring and auditing. Under this view, the compliance professionals are the best group to build and run the privacy program because training, auditing and other related activities are compliance skill sets, not necessarily legal skills sets.

This approach treats privacy as one risk area among many different risk areas addressed by a compliance team. One benefit of this approach is that the components of a compliance program, including policies and procedures, training, auditing and monitoring, and risk assessment, can be leveraged for the privacy program. Another benefit is that it strengthens privilege for the privacy legal work. If the legal team both provides privacy legal advice and operationalizes that advice, it may be more difficult to assert privilege over the legal work because it is not cleanly separated from nonlegal work. Separating privacy legal and privacy compliance creates a clear dividing line between legal and nonlegal work.

Legal

On the other hand, this delineation may confuse the business. How should they know when to go to privacy legal with a question and when to go to privacy compliance? It is difficult enough for professionals to draw this line. Asking business stakeholders to do this may be a recipe for confusion. It is simpler for business stakeholders to have just one group answer all privacy questions.

More fundamentally, privacy legal and privacy compliance are so intertwined it may be difficult to separate such work into two groups. If privacy legal simply hands off legal requirements to privacy compliance for implementation, privacy legal could lose the direct connection to the business, not have as deep an understanding of the business facts and, thus, provide less tailored privacy legal advice.

Legal advice is better if it's closely connected to the implementation of that advice. As an example, consider privacy incident investigations. If the privacy team reports to the legal department, it can both conduct the factual investigation of the incident and counsel the legal department, such as under state and federal breach notification laws. If the privacy team reports to the compliance department, it would not advise the company on legal options with respect to privacy, and there would be two groups in charge of responding to the incident.

Information technology or product management

Other possible, though less common, reporting lines for privacy teams are IT or security overseen by the chief information officer or chief information security officer and product management. If the privacy team is under IT or security, it is usually because the CIO or CISO was previously tasked with getting the company's privacy compliance posture to an acceptable position. This is common where the organization's biggest concern is the technical implementation of privacy controls, such as keeping health data within a certain jurisdiction, cookie compliance and automated choice management. If the privacy function is under product management, it could be because privacy is fundamental to the success of the product. This is common in small to medium-sized health technology companies. In larger organizations, there is sometimes a small privacy team under every major product and a central team reporting to another group leveraged by the product privacy teams.

Conclusion

There is no one right answer for the reporting structure, as it will heavily depend on the organization. For example, if an organization has a thriving compliance team and a privacy lawyer who is an expert on the law, but is not skilled in its practical implementation, it may make sense for privacy compliance to be separate from privacy legal. On the other hand, if the compliance team's primary focus is on other areas, such as health care fraud and abuse laws, and the privacy legal team has expertise on privacy implementation, it may make sense to roll all privacy compliance work into privacy legal. The preferred reporting structure for privacy may change over time as a company grows, launches new product lines, and adds or loses key talent.

Different types of health care organizations

Above we described the general scope of work for a health care privacy team in seven core pillars. But the allocation of work between these pillars and the importance of each pillar to the privacy team will depend on the type of organization processing the health information. Below we list the different types of organizations that process health information and describe specific focus areas for each type.

Health plans

Among health care organizations, health plans likely have the most personally identifiable health information. They receive information from pharmacies, health systems, independent doctor/dentist offices, clinical labs and other health care organizations. As a result, they often have the largest privacy teams among health care organizations. Health plans are covered entities under HIPAA and controllers under the EU General Data Protection Regulation, though they often have or own lines of business that function as business associates or processors.

Dental plans

Dental plans are often structured the same as health plans but have fewer people doing privacy work because they tend to be smaller organizations with, historically, less scrutiny of their privacy practices. Dental plans also generally receive less sensitive personally identifiable health information than health plans. Dental plans are covered entities under HIPAA and controllers under the GDPR.

Pharmacies

Large pharmacy chains rival health plans in the size and scope of their privacy programs. Many leverage robust privacy programs from retail parent companies such as Walmart and Target. Smaller pharmacy chains tend to have smaller privacy teams. Nevertheless, pharmacies tend to have some of the most sensitive personally identifiable health information since prescriptions are often required for sensitive treatments. Pharmacies are covered entities under HIPAA and controllers under the GDPR.

Health systems

Health systems are organizations that typically have some combination of hospitals, general clinics, specialty clinics, labs, research centers and pharmacies. They tend to be designed so individuals can get all their health-related services within the system. As a result, health systems tend to have some of the most complete health profiles of individuals. The size and scope of privacy programs at large multistate health systems tend to rival those of large health plans. Health systems are covered entities under HIPAA and controllers under the GDPR.

Academic medical centers

Academic medical centers are health care entities affiliated with medical schools. They tend to have a heavy focus on research, partnerships with other health care organizations, i.e., data sharing, and teaching. Their privacy teams often focus on privacy issues related to medical research. Academic medical centers are covered entities under HIPAA and controllers under the GDPR.

Independent pharmacies, doctor's and dentist's offices

These tend to be the least sophisticated organizations when it comes to privacy programs. The office manager, lead clinician or owner tends to hold the role of privacy officer, whether or not they have strong privacy knowledge. There is rarely a person in the organization with expertise in privacy, and the owner often relies on industry guidance and peers to handle privacy issues such as notices, forms and facility practices. Also, if the office employs a managed services provider for the practice's administrative aspects, that service often provides specific guidance around key privacy topics. Independent pharmacies and medical offices are covered entities under HIPAA and controllers under the GDPR.

Clinical labs

Clinical labs are organizations that provide health-related tests, drug tests, etc. Clinics, hospitals and doctor's offices often collect samples and send them to these organizations for processing. Larger clinical labs tend to have a significant amount of health information and, during the COVID-19 pandemic, many new labs opened. The privacy teams at labs tend to be small. Clinical labs are typically covered entities under HIPAA and controllers under the GDPR.

Medical device and pharmaceutical companies

Medical device and pharmaceutical companies tend to have deidentified or pseudonymized patient information. Hence, the volume of identifiable health information is typically low. They are generally not subject to HIPAA because deidentified data falls outside the scope of the law. However, medical device and pharmaceutical companies are subject to the GDPR because pseudonymous data is still in its scope. As a result, these companies tend to have formal privacy programs though the teams are typically small.

Health care technology companies

There are a wide range of health care technology companies that specifically process health information and provide services to health care organizations. These are frequently business associates under HIPAA and processors under the GDPR. They tend to have small privacy teams, perhaps consisting of a technologist, program manager and/or lawyer. However, when affiliated with large health care or technology companies, they tend to have robust privacy programs.

General technology companies

There are a whole range of technology companies that provide technology services to health care customers, but also serve other industries, such as financial services, retail and manufacturing. This category of companies typically does not build health-care-specific solutions but rather general technology solutions leveraged by health care companies. These are frequently considered business associates under HIPAA and processors under the GDPR. They frequently lack health care privacy expertise but have mature security, contracting processes and technology.

Key challenges and proposed solutions

CHALLENGE

Value of privacy is intangible

One challenge for a privacy team is the value it provides to the organization may not always be tangible or concrete. The privacy discipline does not have well-developed metrics and it can be hard to explain a privacy team's output. More significantly, privacy may be viewed as slowing down or limiting business opportunities involving the use of health information. Moreover, except for perhaps the largest of companies, the potential for regulatory penalties is viewed by businesses as unlikely. As a result, it may be difficult for business teams to understand why privacy is important and how a privacy team should be evaluated. The privacy team should take steps to ensure the business understands the importance of privacy to the organization and provide metrics to measure its performance.

PROPOSED SOLUTIONS

Establish privacy as a business enabler

The most important way to show privacy's value is to establish it as a business enabler. Privacy teams need to make the case to business leaders that a strong privacy program can advance business objectives and, more directly, help the company grow its revenue. To do this, privacy teams need to find a way to tie their work to key business objectives. Tying privacy objectives to broader business objectives will be easier in some companies than in others.

For example, sales and leadership teams at cloud providers that serve health care customers know privacy is important both to win new customers and retain existing ones. Addressing a customer's privacy concerns, both in the due diligence and contracting phases, may be critical to winning their business. The role of health care privacy counsel in cloud companies is to help customers understand how to use the cloud product in compliance with health care privacy laws. The role of such attorneys is not to give customers legal advice but to describe available features that may help them use the tool in compliance with the applicable laws. The privacy team supports the sales team in delivering the right customer messaging. In part, it signals to customers that the company knows what it is doing with health information, it is trustworthy and it is responsible.

There are other ways for the privacy team to demonstrate it is a business enabler. Examples include:

- Creating one-pagers and other customer-friendly collateral to share with potential customers, patients, regulators and key opinion formers.
- Improving privacy-related forms, processes and talking points to speed up the check-in process and increase consent to research and/or marketing.
- Streamlining deidentification and anonymization processes.
- Building relationships with privacy regulators and privacy leaders at key clients.
- Providing easy-to-follow playbooks to those negotiating privacy terms.
- Creating strong alignment with security and legal to ensure a singular view on the technical, administrative and contractual actions designed to protect personal or health information.
- Setting up office hours or other mechanisms for the business to get quick responses to urgent questions.

- Creating clear rules on how health information can be used, by who and for what.

- Working with technologists to automate privacy and security controls where possible.

- Tracking and owning the quick resolution of identified privacy-related challenges the business has flagged and proactively addressing issues that are not yet flagged.

Create and track outcome metrics
A privacy team needs to create and track metrics to measure its performance for the organization. There are two broad types of metrics: activity metrics and outcome metrics. Activity metrics measure the activity of a privacy program. Examples include numbers of:

- Completed privacy impact assessments or data protection impact assessments.

- BAAs completed in the last quarter.

- Vendors for which privacy diligence was completed.

- Privacy complaints or privacy incidents.

- Data subject access requests.

It is common for privacy teams to measure and report on activity metrics, as illustrated by the above examples. But the activity of a privacy team does not equate to its value. A privacy function could perform scores of privacy impact assessments, but the assessments may not result in any substantive privacy changes or improvements to the assessed product. Indeed, a large number of assessments may obscure key risk areas for the company because the privacy team is so awash in assessments that it loses sight of the truly important privacy issues. If a privacy team does not have the influence in the organization to impact the most important privacy issues, it may focus on sheer volume and less controversial topics as an alternative.

Activity metrics may be relevant in supporting the case for a new headcount. If the privacy team shows it supported and responded to 100 privacy incidents and 500 data subject access requests, and it is legally required for the company to respond to such matters on a timely basis, the metric could support a request for an additional headcount.

Outcome metrics, by contrast, are specific outcomes within a company that are driven or supported by the privacy team. They can be tied to business priorities and are often cross functional. They are preferable to activity metrics, but are harder to define and track. Examples of outcome metrics include:

- Improving the speed of privacy review completion by X percentage.

    - The broader business objective is to reduce delays in releasing products. To support this metric, the privacy team would look at what its review entails. Is the process too complicated? Are there additional self-service tools the privacy team could provide to the business? By asking these questions, the privacy team is focused on what contributes to another executive's success (quickly releasing products). A privacy team cannot single-handedly reduce delays to deliver products, as there could be other sources or teams responsible for delays. But if the team can speed up its review, it supports the overall goal of reducing the time for new products to reach the market.

- Reducing privacy bugs/issues found in new products after launch by Y percentage.

    - This metric is tied to the broader business objective of building high-quality products without bugs or issues. This metric is about making the privacy review more effective. Can a privacy team provide better training to product and engineering teams? Are there privacy software tools the company can leverage? Overall, how can the company deliver products with robust privacy functionality built in? This metric is hard to define and measure, but it is relevant and important to the business.

- Increasing percentage of contracts that have a BAA, where needed.
    - This is an outcome metric because it shows how well the privacy team and other legal teams are doing to put BAAs in place where needed. It focuses not on the activities of the privacy team but on the results of their activities. An activity metric, by contrast, would look at how many BAAs the privacy team supported. But this latter metric does not show how well the privacy team performs, it just shows pure volume. Note this outcome metric is more difficult to measure and track than the activity metric.

Below are additional examples of outcome metrics to consider:

- Percentage of privacy notices (website, application, notice of privacy practices, etc.) reviewed in the last 12 months.
- Percentage of existing employees and contractors that took the annual privacy training in the last 12 months.
- Percentage of data subject access requests or individual rights requests satisfied within X number of days.
- Percentage of new medium and high-risk privacy-related audit findings mitigated or resolved within X number of months.
- Percentage of privacy incidents, opened in the last 12 months, resolved in 30 days or less.
- Percentage of external facing applications/products with active security and privacy certifications (ISO 27001, ISO 27017, ISO 27018, SOC 2-Type 2HITRUST).
- Percentage of active privacy agreements, including BAAs and data processing agreements with desired terms, such as the right language on data rights, breach notifications and indemnification.

CHALLENGE

Privacy team is small

Privacy teams are generally very small parts of the organizations they serve. This is true even for organizations that process health information and look to undertake novel and innovative projects with that data. Yet the scope of work a privacy team assumes is large, given the variety and sheer number of global, federal and local privacy, or privacy-impacting, laws.

Even when compared to the rest of the legal team, the privacy team is generally quite small and grows more slowly than commercial legal, procurement legal, product counsel and other teams within legal. Many in-house legal teams have one primary client. For example, commercial legal teams support the sales organization, employment counsel teams support human resources, mergers and acquisitions legal teams support M&A business teams and product counsel supports the product teams. As these business teams grow, the corresponding legal team will often grow to support them. The privacy team, by contrast, does not have just one internal client. It supports sales, product, HR, M&A and many other business teams. Privacy also supports the legal team. Because the privacy team does not have one primary client within an organization, there is not one business team to which it can tie its growth in headcount.

In sum, the privacy team headcount can be expected to stay relatively small compared to other legal teams. The privacy team needs to think about how it can exert the maximum influence given its small size.

PROPOSED SOLUTIONS

Advocate for needed headcount

The first solution to address this issue is to grow the size of the privacy team. While it is possible to leverage other teams, including product counsel and commercial legal, to extend the privacy team's influence, this leverage has its limits. The primary job for these other teams is not privacy. No team will be more effective at influencing privacy than the privacy team itself. A small privacy team will be limited in how much commercial support can be provided in engaging with product teams, conducting vendor reviews, preparing detailed privacy documentation and supporting incidents. All these activities take boots-on-the-ground privacy personnel.

More significantly, for privacy teams to make an impact and demonstrate value, they need to swing for home runs. A small privacy team can do the bread-and-butter privacy compliance, including making sure the company has the right policies and procedures, meets all the basic regulatory requirements and handles incidents the right way. This could constitute a viable and valuable privacy office, mainly from a risk mitigation perspective. But a privacy team can significantly enhance its value to an organization by helping it understand the health information it has and identifying pathways to grow and improve the business using the data. To do this, the privacy team will need to implement a program to adequately manage the usage and rights of this data. It is an investment that will require more than a few people to manage compliance risks.

A. Making the case

To effectively advocate for a new privacy headcount, a privacy leader first needs to have a deep conversation with each member of the privacy team and inventory all work completed by each team member and the team collectively. As part of this conversation, ask team members:

- Is there a universe of privacy work you're not doing?
- If so, is it not being completed or is it completed by someone else?
- Are product managers or other nonprivacy personnel making the call on privacy topics?
- Have there been any issues identified the privacy team is not able to review?
- If so, did that lead to any customer questions or issues?

From these discussions, describe what the privacy team is and is not able to handle with its current staff and the impact to the organization. For example, one finding might be, with current staffing, the privacy team is able to support major product launches but is not able to support incremental changes. If the privacy team does not have the bandwidth to handle incremental product changes, such products may get released with privacy issues. If the goal of the company is to deliver flawless products, more privacy resources are needed to ensure the privacy team has enough power to support review of incremental product changes.

Beyond the current state, the other data point for headcount planning is the future of the business. Look at planned customer growth. Then look at privacy needs to support that growth. For example, suppose a privacy team member needs to be heavily involved in customer implementations of a software product. Assume a team member can support a total of 10 customers at a time for implementation. If the year's business objective is to add 20 new customers, and the current privacy team is already fully allocated, then the privacy team needs to add two new team members to support planned customer growth. The key here is to tie privacy headcount to business objectives.

Advocating for headcount is a business school-like effort and the output should be a document or deck that lays out the case. It will have lots of numbers and extrapolations. Even where the data is not hard data, try to have a logical extrapolation for how it was calculated. There should be very little talk about regulatory risk. There should be an assumption section that says the company wants to comply with all laws and agreements. Ideally the privacy leader delivers the written pitch. While having the facts and numbers in a deck is persuasive, the message is best delivered by the privacy leader because they will have the most passion about the topic. It is also helpful when the privacy leader has the buy-in from their supervisor. If the general counsel, head of product or compliance officer can articulate that additional resources are needed to best support the legal, product or compliance departments, then the resource request is more likely to succeed.

Create specialized subteams

Even with a small team, if the team is effectively organized, it can be more influential and effective. One way to structure a privacy team, assuming it has sufficient size, is to break the team down into four distinct areas of experience: privacy legal, privacy compliance, privacy operations and privacy engineering. We describe what each of these areas may cover in such a structure and discuss how the four subteams work together below. Note, in many organizations these four areas may not all report to the head of privacy. For example, a privacy engineering team may report to the head of product or the head of engineering. But it is ideal if all four subteams are on one combined team, given the substantial areas of overlap and coordination between them. At a minimum, privacy engineering, privacy legal, privacy compliance and privacy operations should establish a regular operating mechanism to help them work closely together.

A. Privacy legal

The privacy legal team should be responsible for:

- Negotiating data processing agreements, BAAs, and other privacy or security exhibits or agreements. The privacy legal team may directly negotiate the privacy and security terms or it may delegate all standard data processing agreements and BAAs to the commercial legal team and handle all escalations or particularly challenging negotiations.

- Negotiating, or working closely with the security team to negotiate, the security addenda.

- Developing white papers, summary sheets or one-pagers on compliance with the GDPR, HIPAA and other laws, including white papers on data transfer impact assessments.

- Performing M&A privacy due diligence.

- Managing escalated privacy and security incidents. Assume there are three tiers of incidents, where green is the least serious, yellow is medium and red is the most serious. The privacy legal team could handle all the red incidents while privacy operations could handle the green and yellow incidents.

- Analyzing each new privacy law and any new decisions a regulator publishes.
- Working with outside counsel to conduct jurisdictional overviews.
- Working with public affairs to conduct any lobbying.
- Serving as the primary privacy contact for all other lawyers in the organization.
- Reviewing all externally facing privacy material, such as privacy notices, website statements and privacy white papers.
- Reviewing or submitting any regulatory or government filings.

B. Privacy compliance

The privacy compliance team should be responsible for:

- Responding to customer privacy assessments and answering data-protection questionnaires from customers and prospects.
- Conducting all internal privacy assessments, including assessments related to compliance with applicable law, and working with internal audit to coordinate audits related to privacy.
- Managing remediation of audit findings.
- Working with the security team to make sure all the security assessments, both internal and external, are completed.
- Conducting vendor assessments.
- Drafting policies and procedures, and auditing implementation of policies and procedures.
- Managing the privacy training program.
- Translating memos and guidance from privacy legal into policies and procedures that can be implemented by the organization.
- Working with privacy engineering to make sure the organization's PbD program supports compliance with privacy policies, procedures and applicable laws for products and services.

C. Privacy operations

The privacy operations team should be responsible for:

- Creating privacy policies and procedures in coordination with the privacy compliance team.
- Implementing policies and procedures throughout the organization by working with the business functions to incorporate the requirements of policies and procedures into business practices.
- Serving as the front door to privacy for the business. When they have any privacy questions, they come to the privacy operations team. Privacy operations may punt to the privacy legal and privacy compliance teams on certain areas, but it remains the point of contact for the business. Its job is to help all the businesses be successful at implementing privacy requirements within their operations.

- Handling all green and yellow privacy and security incidents, as mentioned in the explanation of the privacy legal team.

- Responding to individual privacy rights requests, i.e., data subject access requests.

- Working with the marketing team around technology issues related to the consent management program and cookies.

- Project managing most privacy initiatives.

- Managing integrations related to M&A activities.

- Managing any privacy tools, registrations and memberships.

- Responding to general privacy mailbox inquiries and complaints.

D. Privacy engineering

The privacy engineering team should be responsible for:

- Working with product and technology teams, as the technology branch of the privacy team. This team is typically not comprised of lawyers, is more technically savy and speaks the same language as product managers and engineers.

- Incorporating privacy into technology and implementing PbD in external products and services, and internal uses of technology.

- Creating checklists, in coordination with the privacy compliance team, for the product teams to help address privacy on projects. Product managers can reference the checklist on each project to make sure they satisfy key privacy requirements. If they can't, they should talk to the privacy engineering team.

- Syncing with the product teams and providing them with regular training.

- Maintaining awareness of discovered privacy and security vulnerabilities in the organization's technologies.

E. Combined team

The structure described above represents a cohesive and cross-functional privacy team, including each part of the privacy ecosystem. The benefit of this approach is that these four expert areas are part of the same team. If privacy engineering sits within the engineering or product organization functions, it will not be as closely synced with other privacy subteams. With this structure, all four areas are closely aligned and meet regularly. Also, this approach creates a leadership structure for a privacy leader. The privacy leader can look to the leader of each subteam to think about and drive the vision to make that subteam successful. The challenges and solutions for each of these areas may be very different. With this structure, the leader can focus on how the four functions work together.

The other benefit of this approach is that there are clear lines for the business about where to go for privacy help. Any questions on operations go to the head of the privacy operations team. For the IT team, all privacy questions should go to the privacy engineering team. All privacy questions for internal audit, procurement and security compliance teams should go to the privacy compliance team. And for the legal team, all privacy questions should go straight to the privacy legal team. This is a simplified message for stakeholders throughout the organization.

Also, the structure provides an example of privacy defense in depth. The privacy operations and privacy engineering teams are the first line of defense. They make sure things get done from the beginning. Privacy compliance is a second line of defense. They check that the business adheres to policies and procedures on a frequent and proactive basis. Internal audit is an additional line of defense. Ideally, if the privacy compliance team is checking frequently and monitoring compliance, then internal audit will find fewer issues when it conducts privacy audits.

In terms of the makeup of the team, privacy compliance and privacy legal subteams will typically be comprised of lawyers and other legal professionals. Privacy operations and privacy engineering subteams tend to have individuals with strong technical backgrounds and good privacy knowledge. The privacy legal team will interact most closely with the privacy compliance team. The privacy operations team tends to work with all functions but mostly escalates matters to the privacy legal team. The privacy engineering team tends to escalate matters to the privacy compliance team.

One downside of the above organizational approach is that team members could get siloed, bored or burned out focusing on just one specific area or activity, such as incidents. Individuals may want to develop their expertise holistically and be skilled in a wide range of privacy areas. Thus, there may be retention issues with team members if they think their focus is getting too narrow. One way to address this is to move team members within the groups, so someone could do a two-year stint in privacy legal, then move to privacy compliance and so on. Also, even within a particular subteam, there are different activities, so it may be possible to keep an individual on the subteam while giving them a broader range of activities.

If a company does not have enough individuals to create four distinct subteams, it could organize its team as follows:

- Option 0: The default recommended team design as described above.
    - Privacy leader.
        - Privacy legal.
        - Privacy compliance.
        - Privacy operations.
        - Privacy engineering.
- Option 1: Best for a small team with 50/50 legal/technical mix.
    - Privacy leader.
        - Privacy governance, includes legal and compliance.
        - Privacy operations, includes operations and engineering.
- Option 2: Best for a small team that leans legal.
    - Privacy leader
        - Privacy legal, includes legal and operations.
        - Privacy compliance, includes compliance and engineering.
- Option 3: Best for medium-size teams handling a large number of agreements or external requests.
    - Privacy leader.
        - Privacy legal.

        - Privacy compliance.
        - Privacy operations, includes operations and engineering.
- Option 4: Best for medium-size teams that do a lot of privacy engineering work.
    - Privacy leader
        - Privacy legal, includes legal and operations.
        - Privacy compliance.
        - Privacy engineering.

Focus on procedures

A small privacy team should focus on high-leverage activities. Well-drafted privacy procedures can be one of the highest-leverage activities for a privacy team and can serve as the foundation for a good privacy program.

Privacy policies look like a restatement of the legal requirements. They are basically made for lawyers to pass external audits and are not very useful to a privacy team. Procedures, however, are the secret sauce for a privacy team. They should be simple, concrete, bulleted checklists. They should help people figure out how to do their jobs in practical, plain terms, avoiding legalese or any unnecessary language. They should be directed to particular teams or activities.

By making procedures simple, the privacy team will intentionally skip important nuances. It is more important to get things right 90% of the time, then detect the other 10%, when additional privacy analysis or work is needed, on the back end. If a procedure tries to cover 100% of the use cases, it becomes so complex the business cannot function without privacy support. That becomes resource intensive and privacy becomes a bottleneck, particularly when the privacy team is small.

Rely on key partners

As privacy teams are heavily dependent on other teams to achieve their goals, they must have strong relationships with company leaders, including heads of sales, marketing and product. Without strong, collaborative relationships with other teams, privacy operates in a vacuum. This is purgatory for a privacy team: procedures are written but not followed, product feature changes are recommended but not implemented, privacy incidents occur but are not escalated appropriately.

Below we discuss key partners who help extend the influence of privacy and help the privacy team meet its objectives. At the same time, the privacy team supports these teams and helps them meet their own objectives.

A. Legal

The legal team, across many different areas, is a critical partner to the privacy team. In this section, we discuss key areas of intersection between privacy and members of the legal team.

1. Commercial legal

The commercial legal team is critical to privacy because it is tasked with negotiating agreements, including privacy agreements, with customers. It is also often the company's primary legal voice on privacy topics toward customers. While the privacy team may directly negotiate some privacy agreements, in general they provide back-end support to the commercial legal team on customer privacy negotiations. The commercial legal team will likely field persistent privacy questions from customers on topics including international transfers of health information, secondary uses of data, breach notifications and audit rights.

A customer privacy negotiation playbook should be the heart of the collaboration between commercial legal and privacy teams. The playbook should provide all privacy information the commercial legal team needs, including descriptions of the privacy exhibits/agreements offered to customers, information on how to answer difficult and detailed privacy questions, suggested fallback language and escalation paths to resolve issues. The playbook should continually evolve and improve to address new issues, product changes, legal changes, or changes in a company's approach or strategy. The commercial legal team should be a key contributor by raising questions for the playbook to address and providing feedback on which approaches worked well and which did not. As the commercial legal team grows, it will have an immediate resource and starting place for negotiating privacy provisions and will not need extensive privacy training to get started. This is scalable, as commercial legal teams are likely to grow much more quickly than privacy teams and it is important to find a way to provide guidance that can be leveraged many times.

2. Procurement legal

The procurement legal team negotiates vendor contracts for the enterprise. Ensuring vendors are appropriately protecting and securing health information is foundational for a privacy program. Accordingly, the privacy team should rely on and support the procurement legal team regarding vendor privacy diligence and privacy contracting. The procurement legal team will generally negotiate the privacy exhibits and agreements, e.g., data processing agreements and BAAs, and escalate to the privacy team as needed.

The privacy team should create a vendor privacy negotiation playbook for the procurement legal team. It will serve a similar function as the customer privacy negotiation playbook and should link to privacy templates and address common negotiation points. For particularly complex privacy negotiations, the privacy team may directly own the negotiation of privacy exhibits with vendors. The difference, compared to customer negotiations, is that companies are often forced to work off the vendor paper. Thus, the playbook will be more of a checklist of what to look for and revise in the vendor paper, rather than how to negotiate off the company's own agreements.

3. Product counsel

The role of product counsel in organizations, particularly technology companies, is increasingly important. The product counsel team is the first and primary legal point of contact for product managers and engineers. Product counsel personnel act as the arms and legs for privacy in advising product and engineering teams on privacy issues. Also, product counsel is usually the first team within legal to identify new products or services that impact privacy.

The product counsel team supports and advises new product launches and responds to all questions from product managers related to legal matters. After getting the facts from the product managers, the product counsel team identifies the issue and flags the right people to support analysis on the subject.

As part of its outreach to other teams, the product counsel team gives subject matter experts the right level of detail, so they can give crisp assessments. If the subject matter expert does not have sufficient facts or context on the product in question, the advice tends to be more general, though precise guidance would be more helpful.

The product counsel team takes collective feedback from subject matter experts and brings it back to the product team. They break down the substantive legal requirements into concrete requirements product managers can understand and implement. Also, to the extent there are multiple options with different risk profiles, the product counsel team advises the business on the pros and cons for each option under consideration.

On complex privacy matters, it is ideal for the privacy team to be directly engaged with product managers, in coordination with product counsel, to ensure the facts are well understood by the privacy team, and the privacy analysis and guidance is well understood by the product managers.

4. Business unit counsel

Many health care companies do not have a product counsel role and instead have a business unit counsel role, which is a lawyer dedicated to all legal matters for a business unit. The business unit counsel team plays a critical role in implementing a privacy program because, like the product counsel team, they are the closest to business teams with most privacy issues in a company.

Depending on the size of the organization, it is common for business unit lawyers to take privacy requirements from the privacy team and apply that guidance to the business unit. The privacy team may provide resources to the business unit lawyers, such as a memo distilling new requirements under the California Privacy Rights Act, tools or processes to support data subject access requests, and template privacy notices. It is the business unit lawyer's job to take these resources and implement them. The business unit lawyer will be the central point of contact for the business on all privacy questions.

What is the difference between business unit counsel and product counsel? A business unit lawyer generally serves the entire business unit of a company and leads all legal issues for that business unit, whether in employment, contracting, marketing or product counseling. This lawyer's main client is the head of the business unit. A product lawyer, by contract, typically focuses on advising product and engineering teams on new products and services.

B. Information security

A privacy team's closest partner outside of legal is the information security team. Privacy and security laws and requirements are heavily interdependent: privacy laws contain security requirements and security laws contain privacy requirements. The head of privacy and head of security should be in continuous communication to align on internal audits, incident responses and vendor assessments. The security team primarily focuses on the confidentiality, integrity and availability of data, while the privacy team focuses on how properly secured data is used. In smaller organizations, the privacy and security leaders are often the same person. Also, in many organizations, including some large organizations, the privacy counsel and cybersecurity counsel are often the same person.

As an example of collaboration, companies may have a security compliance team that manages their certifications and accreditations, Service Organization Controls 2, Payment Card Industry Data Security Standards Council and International Organization for Standardization. The privacy team may have a point person, ideally someone with a background in security and privacy auditing, to work with the security compliance team on areas of certification that require privacy support, such as the implementation of privacy and security controls throughout the enterprise. The privacy team also serves as a translator between what the customer demands on certifications and what the company offers.

Another important area of collaboration is vendor assessments. Information security tends to lead the work on vendor assessments because the focus is more security intensive than privacy intensive. The privacy team can help ensure the appropriate privacy agreements are in place and the vendor's use of health information is appropriately limited.

Effectively prioritize

Despite the above efforts, many privacy teams will not have the bandwidth to complete all possible privacy projects. Thus, privacy teams need to prioritize efforts with the most impact. Effective prioritization may mean the difference between a high-leverage, impactful team versus one that gets bogged down in projects of lesser importance to an organization.

The basic idea of prioritization is to create a complete list of the privacy team's possible projects/activities and evaluate its available resources, then determine the projects/activities it can complete and those it cannot complete. But how should a team prioritize its efforts?

As a first filter, one approach is to prioritize external commitments. These may include commitments to regulators, customers, privacy notices and policies, and other areas where a company makes external commitments related to its privacy program. Regulatory commitments made by the company above and beyond normal legal requirements, such as a consent decree or regulatory conditions to a merger, should be at the top of the list. They must get done.

The next level of priority should focus on the company's product and services. One approach is to prioritize consumer-facing products first, then business-to-business products. A privacy team may be the only gatekeeper for protecting individual privacy for consumer products. B2B products often have another set of eyes, e.g., the business customer, to evaluate privacy compliance.

Then, look at the company's business priorities to find other high-priority privacy projects.

To further refine the prioritization list, evaluate whether, for the identified in-scope projects/activities, another competent person on the project can represent the interests and views of the privacy team. If so, the privacy team can deprioritize the project.

There may also be a range of legally required items a privacy team does not have time to complete. The privacy team should flag them, and work with the compliance team and business leadership to determine the best course of action.

CHALLENGE

Privacy by design is difficult to successfully implement

PbD is often touted as the key way to build a strong privacy program. If the privacy team can get involved in projects early, provide input and be a key stakeholder throughout the product development lifecycle, then privacy-preserving products will result. The reality is PbD is hard to get right and privacy teams continuously struggle to find the right balance between sitting in on every product team meeting versus learning about a product feature a day before its launch.

One of the key challenges of PbD is that privacy teams speak a different language than product managers and engineers. Product managers and engineers look for specific and concrete requirements for satisfying privacy requirements. But privacy laws like the GDPR and CPRA are not written prescriptively, to tell you exactly what to do, but are principle based. Thus, it can be difficult for a privacy team to deliver the black and white rules product managers and engineers seek. Below we discuss two solutions that could help implement PbD in an organization.

PROPOSED SOLUTIONS

Build relationships with product organization

The first step to successfully implementing PbD is building strong relationships with the product organization.

To start, define the key stakeholders within the product organization. Product managers facilitate the building of the product without doing the actual building. Product managers gather requirements, speak to customers and create product strategies. They then drive the work to build the products on the roadmap. Product managers work with engineers, marketing, sales, go-to-market teams and finance. Their closest partners are the engineers who write the code and build the product. Thus, the key stakeholders for PbD programs are product managers and engineers.

The next step is to figure out which team within legal will have the primary relationships with the product managers and engineers on privacy matters. The three primary candidates are the privacy, product counsel and business unit counsel teams. We will assume for the rest of this discussion the company has a product counsel team, but where a product counsel team does not exist, either the privacy counsel or business unit counsel team can take the steps described below.

The product counsel team is the connection between the privacy and product teams. The primary role for the product counsel team is to review new products and features from a legal perspective. To support such review, the product counsel team may develop a privacy checklist, in coordination with the privacy team, to help them recognize and get information from the product managers and engineers about sensitive privacy issues. The checklist may not be a set of requirements but rather a list of high-level questions to help probe the product managers on their actions and potential product changes. The checklist may ask:

- Does the product collect health information or other personal information?
- If so, why is it being collected? For what uses?
- Are there subcontractors? What are they using it for?
- Will the health information be transferred to another jurisdiction?
- How long will data be retained?
- If someone wants to delete data, what happens?
- What questions will we get from customers?
- Does the product really need the data it is getting? If the data is being shared with someone, does the data subject know about it?
- Are there unintended consequences of data processing? Does the product collect a new data store, upgrade to a new environment or country, or make new uses of existing data?

The checklist supports the relationship between the product managers and the product counsel team. But no checklist or tool can replace the value of the conversation between the product managers and the product counsel team (and privacy counsel where appropriate) to support the product counsel's understanding of the product and the product managers' understanding of the legal and contractual constraints related to that product.

If the product-review process is automatic or does not provide that level of education, then the product teams will not necessarily learn anything more about privacy.

The high-level checklist above is not a replacement for full-blown privacy impact assessment conducted by the privacy team, if triggered.

Create an easy path

The goal of the privacy team is to be scalable and not block business. Engineering and product teams may see the privacy team as another gate and blocker, but the privacy team can take steps to avoid this. Perhaps an ideal state is where product managers can launch products that are privacy aware but do not require more work for their team, as the privacy features are automatically built in. The privacy bolt-on is the real problem from the product and engineering standpoint. How does a privacy team get closer to this idealized state?

The answer is to create an easy path for product managers to launch products. This path is the most straightforward and clean from a privacy perspective. If the product manager takes the easy path, the privacy review will be streamlined. For example, the easy path might say, for new data processing needs, create a virtual private cloud with built-in privacy configurations, rather than spinning up an entirely new cloud that would require additional privacy work. This provides product managers and engineers with the mechanism to have as little privacy friction as possible.

If the easy path is unavailable because it is a blocker or technical problem, then consult with the product counsel team, who will loop in the privacy team. The product counsel and privacy teams can then come up with an alternative and build out additional well-worn paths for product managers. Over time, in addition to administrative guardrails, product managers can create technical guardrails, such as opportunities to automate or put something into the software development release cycle. Under this approach, there would be a technical gating from releasing the product into production without certain features in place. Over time, a privacy team will gain confidence that teams are doing the right thing without being involved in every step. Then the product and privacy teams can focus their efforts on the most cutting-edge issues.

Conclusion

Here is a brief overview of the key insights in this paper. To start, the scope of work for which a privacy team is responsible can be broken down into seven distinct areas:

1. Legal analysis: Analyzing relevant laws and regulations and their applications to the organization.
2. Policies and procedures: Translating the laws and regulations into tangible and concrete guidance a company and its personnel can implement.
3. Contracting: Contracting matters are a key part of a privacy team's job, as privacy laws contain many requirements around contracting.
4. PbD: Ensuring products and services are built with privacy in mind and incorporate privacy requirements.
5. Privacy operations: Ensuring privacy is implemented throughout all aspects of an organization through a diverse set of activities.
6. Privacy risk assessment: Evaluating a company's privacy risks, making plans to address them and following through with regular auditing to ensure risks are appropriately addressed.
7. Security coordination: Coordinating with the security team, as privacy and security overlap and are mutually dependent.

The privacy team typically sits within the legal organization, with a direct reporting line to the general counsel. While the privacy legal team may in some cases be separated from the privacy compliance team, this can be challenging as there is no clear dividing line between legal and compliance matters. Rather, legal, compliance and operational matters tend to be closely related and solved in reference to each other.

There are also different categories of health care organizations that process health information. Different types of organizations interact differently with health information and the individuals to whom the data relates. Some organizations engage directly with patients and may be most focused on scalable ways to support these types of interactions. Other organizations, such as cloud providers, may process massive amounts of health information but may never look at it or engage directly with the patient. Thus, the privacy issues that different types of organizations confront vary widely.

With that foundation, there are three key privacy challenges that confront health care organizations and proposed practical solutions to address these challenges.

CHALLENGE

Value of privacy is intangible

Privacy law is a relatively new field, and its structures, rules and requirements are still under development by regulators and companies alike. Moreover, privacy can be an amorphous concept, and it can be difficult to define exactly what "good privacy" means. There is a lack of established metrics to measure the success of a privacy program. All this collectively means it can be difficult to explain the value and importance of privacy to organizations.

SOLUTIONS

- First, it is important to tie privacy objectives to the larger business objectives. The business needs to believe getting privacy right is a critical business priority. If privacy objectives are not closely tied to business objectives, the privacy team will be less influential and more likely to operate in a siloed and isolated fashion.

- Second, to enable measurement of a privacy team's performance, the team should seek to identify and track key outcome metrics that demonstrate how it supports important outcomes at the company. Activity metrics, which show the activities the privacy team performs, are less useful than outcome metrics.

CHALLENGE

Privacy team is small

The next challenge is that privacy teams are generally small, even within larger organizations that process vast amounts of health information. This makes it harder for the privacy team to meet its objectives and have influence in the organization.

SOLUTIONS

- Advocate for the needed headcount. This is not a skill taught in law school or at privacy conferences but it is an important aspect of leading a privacy program. Make the case for headcount by taking a methodical and data-driven approach.

- Create specialized subteams. Here is one structure for a privacy team consisting of four distinct areas of expertise: privacy legal, privacy compliance, privacy operations and privacy engineering. As the privacy team grows, it's helpful to have a leader in each of these areas, with an overall privacy leader focused on ensuring all areas are coordinated and mutually supported.

- Focus on procedures. Well-crafted procedures are the secret sauce to a good privacy program. They scale well, support consistency and give teams clarity on exactly what steps to take to meet privacy requirements.

- Rely on key partners. To meet their objectives, privacy teams rely heavily on the support of other teams, most notably from the legal team, including commercial legal, procurement legal, product counsel and business unit counsel, and the information security team.

- Effectively prioritize. The privacy team should carefully evaluate the privacy projects that are the most important to the organization. It is likely a privacy team cannot undertake all the projects it would like to, and needs to develop and apply criteria for selecting the most impactful privacy efforts.

CHALLENGE

PbD is difficult to successfully implement

Implementing PbD is frequently cited as best practice by regulators and, in the case of the GDPR, is statutorily required. But implementing PbD effectively, particularly as health care products and services become more data-intensive, is an area that warrants continued focus and attention.

- Build relationships with product organizations. PbD can only happen if the product teams understand the importance of privacy to the organization and its products. In many organizations, the product counsel or business unit counsel teams will have the primary relationships with the product teams. Thus, these lawyers will play a key role in the PbD program.

- Create an easy path. Privacy needs to provide product managers and engineers, as part of product development, with a way to address privacy issues proactively and efficiently. To do this, the privacy team needs to provide easy paths, with the appropriate privacy guardrails built in, to these teams.

Real challenges confront privacy teams when implementing robust health care privacy programs. Privacy laws are changing quickly, and the field of privacy is still in its relative infancy. There is great promise for the use of health information to further the health care ecosystem. At the same time, there is a strong need to protect the privacy of patients and other individuals with respect to their health information. A privacy team's role is to help companies strike the right balance between the two. As described above, the skill set needed for successful in-house privacy counsel to achieve this is as much interpersonal as strictly legal.