Privacy Readiness:

Do you know where your PHI lives with Medical Device companies?

March 31, 2020

Arthrex

1

Introductions

Alison Brunelle
PwC
Director, Privacy & Consumer Protection
alison.brunelle@pwc.com
+1 (512) 626-3435

- Alison is based in PwC's Austin, Texas office. She is a senior corporate consulting leader experienced in building and sustaining enterprise-wide privacy programs. Her multifaceted background as a compliance and risk management professional with legal training and private and public sector experience allows her to solve complex business problems while increasing enterprise value and mitigating risk to highly valued data.
- Previously Alison served as the Privacy Officer for a $24b retailer leading an enterprise privacy program responsible for bringing to bear information governance practices across omnichannel operations that included grocery, health care, ecommerce, gas, and transportation.
- As a recognized longtime privacy practitioner, Alison served at the direction of the appointed Chief Privacy Officer mandated under the Health Information Technology for Economic and Clinical Health (HITECH) Act supporting public policy formulation for safeguarding the privacy and security of protected health information (PHI).
- She has advised clients on California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR) compliance requirements including the implementation of privacy program components to remediate known compliance gaps and mature practices.
- Alison is a Fellow of Information Privacy (FIP), Certified Information Privacy Manager (CIPM), Certified Information Privacy Professional specializing in Government (CIPP/G), and Certified Information Privacy Professional (CIPP/US).

Kay Kay Chan
PwC
Director, Healthcare Compliance
kaykay.chan@pwc.com
+1 (206) 941-9151

- Kay Kay is a Director within the healthcare services Internal Audit, Compliance and Risk Management Solutions (ICRS) practice based in the Pacific Northwest market. She has over 12 years of healthcare operations, health information management, privacy, research compliance, corporate compliance, internal controls and risk management experience
- Prior to joining PwC, she held management roles for corporate compliance and operations across health information management, HIPAA privacy, revenue cycle for health systems, research institutes and large medical groups.
- She has led numerous compliance engagements across the the spectrum of health industries and life sciences clients, evaluating security and privacy internal controls, leading clinical trials audits, assessing compliance programs and developing auditing and monitoring programs over key risk areas.
- She is currently focused on internal audit and healthcare compliance services for a variety of health care providers, payers and new entrants assisting in the evaluation of their internal control environments, performing Compliance program effectiveness, leading operational compliance assessments and transforming risk and Compliance programs.
- Kay Kay holds a Masters of Business Administration (MBA) and Bachelor of Science in Health Informatics and Information Management from the University of Washington. She is certified as a Registered Health Information Administrator (RHIA) and in health care compliance (CHC).

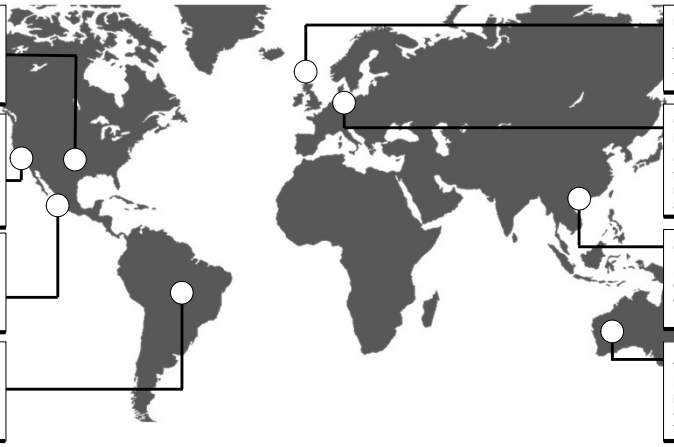
Jason Vendel
Arthrex, Inc.
Senior Manager, Compliance Investigations & Global Privacy

- Jason is the Senior Manager for Compliance Investigations and Global Privacy at Arthrex, Inc., based in Naples, Florida. Jason graduated from Cornell Law School and then served as a law clerk to two U.S. federal judges.
- After his clerkships, Jason worked as an associate in the White Collar Litigation Group at Sidley Austin LLP in Washington, D.C, where he represented individual and corporate clients in internal investigations and before government enforcement authorities in corruption- and compliance-related matters, as well in as antitrust, False Claims Act, and Inspectors General investigations.
- Jason then joined the Law Department at Exxon Mobil Corporation in Houston, Texas, where he similarly represented the company in its government enforcement and anti-corruption matters.
- In his current role at Arthrex, Jason leads compliance investigations and government enforcement matters and heads up the company's global privacy program.

2

The privacy landscape

Once the responsibility of a single department, cybersecurity and privacy now touch every part of the business on a global scale.



Health Insurance Portability and Accountability Act (HIPAA)

Mandates a myriad of privacy, security and breach notification requirements regarding protected health information (PHI)

California Consumer Privacy Act (CCPA)

Designates an array of new rights regarding California residents' personal data, starting with the right to be informed about what kinds of personal data companies have collected

Mexico's Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Applies to private individuals or legal entities that process personal data for commercial use

Brazil Lei Geral de Proteção de Dados (LGPD)

Used Europe's General Data Protection Regulation (GDPR) as the blueprint for a national privacy framework for Brazil

UK Data Protection Act

Aims to modernize data protection laws to make sure they are effective in years to come

General Data Protection Regulation (GDPR)

Gives regulators unprecedented power to impose fines for privacy violations, requiring wide-scale privacy changes across organizations operating in the EU

China Cybersecurity Law

Establishes new requirements for user consent in China, as well as for personal data collection, storage, and sharing

Amendment to Australia Privacy Act

Introduces a mandatory notification procedure for data breaches as an amendment to the existing legislation from 1988

Note: this map is for illustrative purposes only and is not intended to be inclusive of all global privacy laws and regulations.

3

Comparison of key HIPAA requirements against CCPA and GDPR

While HIPAA regulates Protected Health Information (PHI) collected by an organization, the CCPA and GDPR regulate personal information collected by healthcare organizations that is not covered by HIPAA. The differences between each regulations' requirements with respect to patients, consumers and organizations covered by HIPAA are detailed below.

	CCPA		HIPAA		GDPR
Scope	California residents' personal information *collected and processed*	◇◇	Protected Health Information *held*, *processed or transferred within the United States (*including non-United States citizens or residents)	◇◇	EU personal data *processed*
Right to access	Right to access specific personal information, and categories of personal information collected, sold and disclosed about the requesting consumer, within the 12 months preceding their request	◇◇	Right to access certain PHI (that is part of a 'designated record set') for as long as the information is maintained	◇◇	Right to access all EU personal data processed
Right to portability	All access requests must be exported in user-friendly format, but there is no import requirement	><|	Must export the data in the manner requested by the individual (subject to entity in question capabilities and security measures)	><|	Must export and import certain EU personal data in a user-friendly format
Right to correction	Not included in CCPA	✕	Right to correct certain PHI (that is part of a 'designated record set') but in general does not include medical information such as diagnosis	≋	Right to correct errors in EU personal data processed
Right to stop processing	Right to opt-out of selling personal data only; must include opt-out link on website	◇◇	Not included in HIPAA	◇◇	Right to withdraw consent or otherwise stop processing of EU personal data
Right to stop third-party transfer	Right to opt-out of selling personal data to third parties	◇◇	Right to stop the transfer of PHI unless it conflicts with one of HIPAA's 'Permitted Uses'	><| ◇◇	Right to withdraw consent for data transfers involving secondary purposes of special categories of data
Right to erasure	Right to erase personal data collected, under certain conditions	◇◇	No right to erasure	◇◇	Right to erase EU personal data, under certain conditions
Right to equal services and price	Explicitly required	◇◇	Not explicitly required	◇◇	At most, implicitly required
Private right of action damages	Privacy right of action afforded ranging from of $100 to $750 per individual per incident	◇◇	No private right of action	◇◇	No floor or ceiling
Regulator enforcement penalties	No ceiling - $7,500 per intentional violation	◇◇	Based on the level of negligence - $100 to $50,000 per violation (or per record), with a maximum penalty of $1.5 million/year	◇◇	Ceiling of 4% of global annual revenues or €20 million, whichever is greater

><| Narrower than HIPAA ◇◇ Broader than HIPAA ≋ Similar to HIPAA ✕ Absent from CCPA or GDPR

4

Personal data holdings at a medical device company

Privacy regulations and enforcement continue to rise. With CCPA, GDPR, and HIPAA, scrutiny is placed on entities to create effective privacy programs. Compliance may feel like an overwhelming task.

As a medical device company, how do you determine the locations, depth, and scope of your personal data holdings and then develop actionable processes and controls to support continued compliance with applicable privacy laws and regulations?

Which teams have personal information?

Priority teams

- Connected Device
- Research
- Information Technology
- Marketing
- Human Resources
- Accounting & Finance
- Facilities Management
- Medical Education
- Quality Assurance

Customer Service

What categories of personal information?

- Patient/Insured PHI
- Customer SPII / Sensitive Personal Data
- Customer PII
- Employee PII

What regulations are in scope?

- HIPAA
- GDPR
- CCPA
- Global, US federal, and state privacy laws and regulations

What challenges do we face?

- How do we determine what data is collected, how it's used, and how it's shared?
- How do we ensure we are considering all relevant aspects of the business (e.g., do we have a self-funded health plan, perform research or medical education involving cadaveric specimens or human subjects, or operate clinics)?
- How do we determine what data we hold is applicable to which global privacy regulations?
- How do we implement processes to regularly update and maintain our understanding of our personal data holdings?
- How do we protect data throughout its life cycle?
- How do we know what our business partners and regulators expect from a privacy program?
- Do we have the right documentation in place to support our privacy program?
- How do we know our operations are ready for a regulatory inquiry?

5

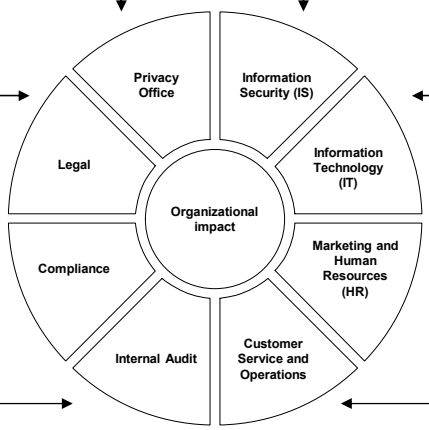
Privacy impacts across the organization

Privacy Office
- Enhancing consumer notice and transparency
- Enforcing privacy by design
- Conducting privacy impact assessments
- Honoring data subject rights

Legal
- Evaluating legal compliance gaps
- Advising on updates and changes to the law
- Managing contract process with third-party sellers, buyers, and processors
- Driving data breach notification
- Managing response to enforcement actions, private and state

Compliance
- Administering corporate policies and procedures, including records retention
- Enforcing privacy requirements across the organization

Internal Audit
- Monitoring and reporting privacy program and compliance
- Promoting continued accountability
- Performing independent assessments of administrative, technical, and physical controls



Information Security (IS)
- Promoting security throughout the data life cycle
- Assisting with data breach notification
- Driving incident response
- Involved in response to civil and state enforcement actions

Information Technology (IT)
- Enabling rights of access and deletion upon identity verification
- Enhancing data life-cycle management functions
- Managing consent indicators and logs
- Maintaining inventory of systems and processing activities

Marketing and Human Resources (HR)
- Limiting data collection and access as a leading practice
- Respecting opt-in and opt-out consent on a rolling basis
- Maintaining standards with third-party sellers, buyers, or processors
- Training employees on privacy compliance

Customer Service and Operations
- Enabling rights of access and deletion
- Fielding questions, inquiries, and concerns while maintaining brand reputation

6

Fireside chat

As a medical device company operating globally and continuing to expand into the connected device market …

What **compliance challenges** are top of mind for Arthrex?

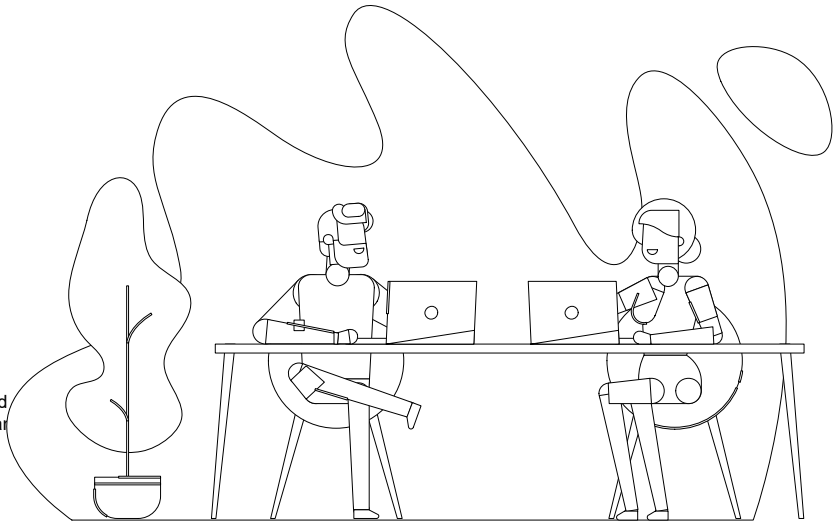
What **surprised** you about Arthrex's personal data holdings?

How is Arthrex developing its **global privacy program**?

How does Arthrex **partner** with its upstream and downstream vendors and third parties, including healthcare systems and provider groups, to:

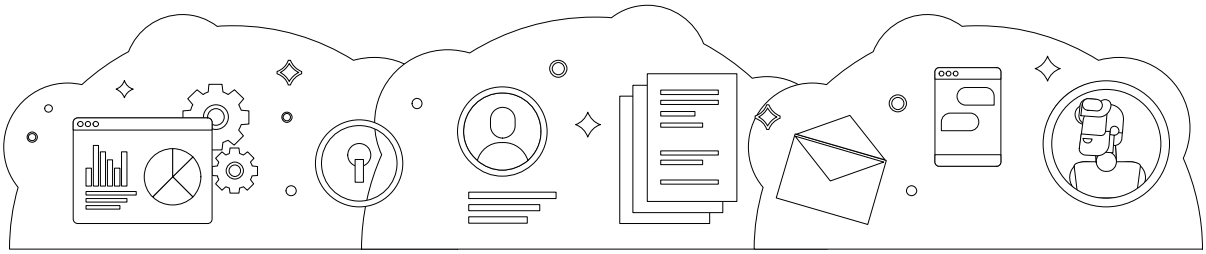
- monitor vendors' privacy compliance, and
- provide assurances of Arthrex's privacy compliance to its partners?

How is Arthrex **planning** for future privacy laws and regulations and changes to the business, such as an expanded connected device portfolio?



7

Key takeaways



Understand your personal data holdings

Assess your operations to determine where and for what purposes you, or your third party partners and vendors on your behalf, are collecting, storing, sharing, and selling personal data. You may be surprised by the types of personal data and business units affected.

Define your privacy program structure

Define the structure and operating approach of the privacy program and its extended members to help ensure compliance:

- Roles in the privacy program
- Privacy champions
- Three lines of defense
- Centralized, advisory, or hybrid model

Monitor regulatory and business changes

Periodically review your privacy program to help ensure it is aligned to current regulatory and business requirements. Implement a process to identify changes to the business that have an impact on privacy processes. Monitor the regulatory environment in the countries where you operate to ensure new privacy requirements are identified and processes are implemented to comply with the requirements.

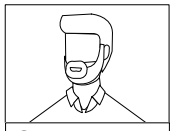
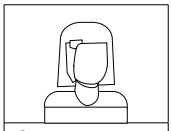
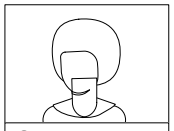
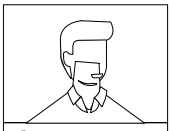
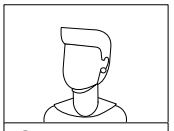
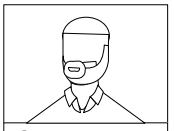
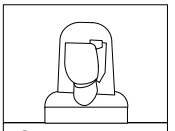
Make privacy capabilities a growth driver, not a barrier

Having a good data strategy and a related effective privacy compliance program can give you a competitive edge. Once you have an understanding of your personal data holdings, build a governance framework to enable risk-based decisions about opportunities to extract value from data while minimizing risk. Design and build privacy and security solutions across the data lifecycle, with alignment to evolving regulations and new technology risks.

8

Key questions about cybersecurity and privacy

Once the responsibility of a single department, cybersecurity and privacy now touch every part of the business.

 **CEO**	 **CRO**	 **CPO**	 **CIO/CISO**	 **Boardroom**	 **CMO**	 **CDO**
Do we understand what the emerging risk landscape means for us?	Do we approach cybersecurity and privacy using a risk-based approach?	Is our organization respecting privacy while monetizing data?	Are we taking appropriate steps to protect our organization against cyber risk?	Do we have the information we need to oversee cybersecurity and privacy risks?	Are we gaining connectivity without losing consumer trust?	Do we have the personal data we need to achieve our business objectives?
Can we articulate our cybersecurity and privacy strategy across the organization?	Can we articulate our current cybersecurity and privacy risks?	Are we following applicable privacy laws and regulations?	Do we measure and demonstrate to stakeholders the effectiveness of our cybersecurity and privacy efforts?	Do we have a tested cyber incident response plan?	Does our program leverage strides in cybersecurity and privacy risk management to boost our economic performance?	Are we acquiring the personal data we need to achieve our business objectives in a compliant and ethical manner? How do we get the most value from our personal data?

9

Thank you

pwc.com

10