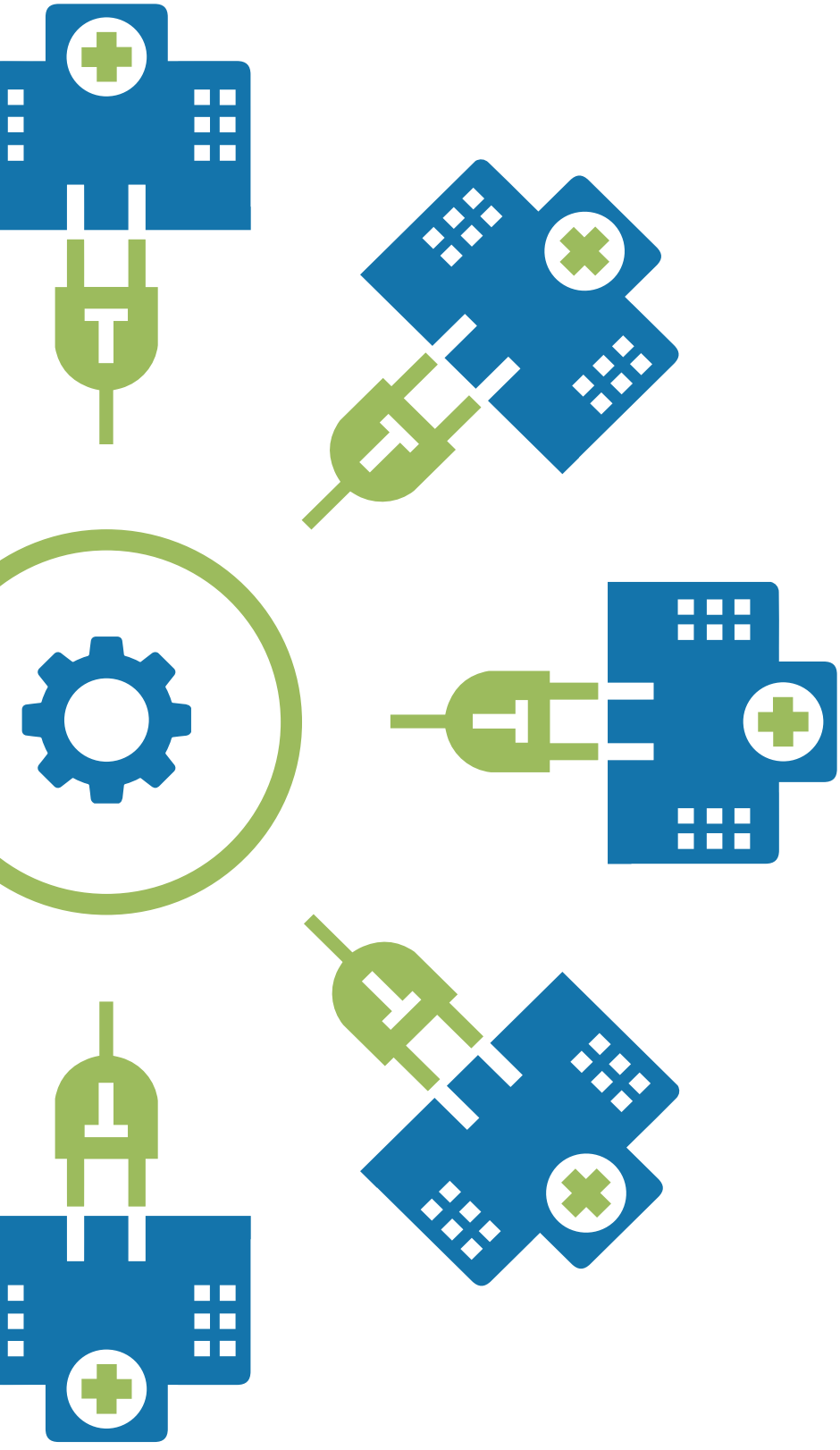
De-Identified Data:
The Competitive Advantage for Medical Devices



PRIVACY ANALYTICS
an IQVIA company

The opportunity

The global medical device market will reach

$409.5 billion by 2023

The challenge

Gaining a competitive edge

while balancing ethical and legal factors

The solution

Responsible data sharing

that powers innovation and new revenue streams

The hyper-competitive medical device market is accelerating

Currently at 4.5% compound annual growth[1], the global market for the medical device industry is accelerating. **Medical device companies with access to the richest data and the ability to deploy innovative data strategies have a clear competitive advantage.** They are better positioned to exploit new opportunities, create shareholder value and withstand pricing pressures as certain sectors become commoditized[2]. These capabilities are highly valuable in the face of growing public scrutiny, the changing legal landscape and the threat of failure from not doing enough[3].

Responsible data sharing for research and development has never been more important. Safe, effective data sharing can advance patient health while providing medical device companies with real-time metrics that validate their product offerings and enhance revenue streams. Patient data must be leveraged for maximum utility – at the lowest possible risk – while demonstrating a proactive approach to personalized treatment insights in the face of market disruptors and insurgents.

Balancing data privacy and utility is the key to a healthy bottom line

As the volume of collected data increases, achieving a balance between data curation and the pressure to meet KPIs becomes ever more complex. Legislation such as HIPAA and GDPR impacts companies' abilities to transport data, both within the organization and across jurisdictions. The introduction of new laws – like the proposed California Consumer Protection Act (CCPA), coupled with the rise in media scrutiny, further compels enterprises to implement best practice in data privacy. The economic impact is already being felt by multinational corporations and publicly held companies[4].

The best, safest, richest data equals competitive advantage

The central question we're asked is how to use data in a way that protects individual privacy, while ensuring that it remains of sufficient quality for useful and meaningful analytics. Our consistent answer is data de-identification. De-identifying data assets supports transformative data strategies which drive innovation, efficiency and revenue.

[1] The global medical device market is expected to reach $409.5 billion by 2023, *lucintel.com, April 2018*

[2] The Growth Imperative for Medical Device Companies, *mckinsey.com, September 2017*

[3] When the human body is the biggest data platform, how will medtechs capture value?, *Ernst & Young, Pulse of the Industry, ey.com, 2018*

[4] The Bottom Line On Trust, *accenture.com, 2018*

Privacy Analytics: a global team of data scientists and business analysts

As pioneers and global leaders in data anonymization techniques for over a decade, Privacy Analytics has set benchmarks for best practice in the management of personal information and protected health information. Our solutions have been proven effective in the most demanding health care environments. Working in consultation with academic institutions, governments, multinationals, and non-profit organizations, Privacy Analytics enables companies to be pro-actively compliant with regulations such as HIPAA, GDPR and others.

	PRIVACY ANALYTICS an IQVIA company	Traditional Masking (Redaction)	Raw Data (Not Anonymized)
HIPAA De-Identification Compliant	✓	✗	✗
GDPR Anonymization Compliant	✓	✗	✗
Risk Level	LOW	MODERATE	HIGH
Data Utility	HIGH	LOW	HIGH

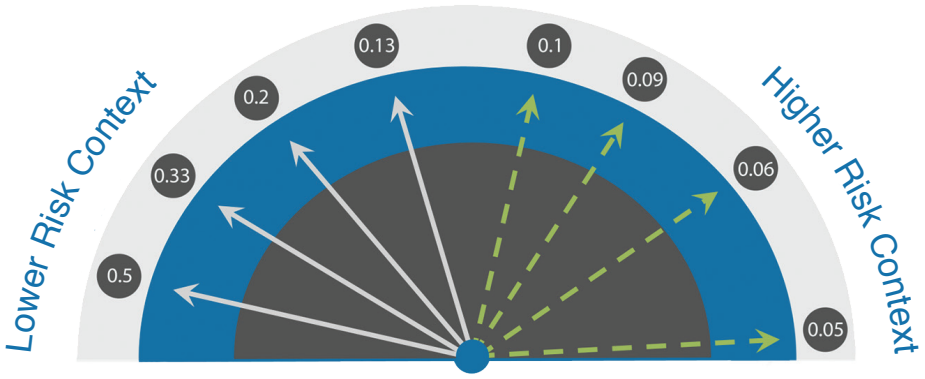
Identifiability exists on a spectrum, and depending on the environment in which data flows different technical solutions may apply. It's important to establish context around the technologies and data flows that will be used in production. In addition to the advantages and limitations of particular technologies, decision makers need to understand where they apply within a deployed pipeline to manage the spectrum of identifiability.

Our clients rely on us as a reputable, trusted, third-party advisor, to help evaluate and mitigate legal barriers related to data ownership and responsibilities. **Privacy Analytics' world-renowned experts in data privacy and responsible sharing are uniquely qualified to deliver on that trust. Our experts are constantly solicited for speaking engagements, conferences and think-tanks around the globe.** They are renowned for pioneering a privacy approach that's recognized by global regulators, and their expertise has informed data-privacy standards around the world.

Privacy Analytics is committed to helping our clients drive healthcare forward and, ultimately, improve human health outcomes. As a wholly-owned subsidiary of IQVIA, the leader in life sciences data sharing with a presence in over 100 countries, **Privacy Analytics' portfolio of solutions contributes to faster and more efficient health research**, using robust real-world evidence to support treatment value, and provide greater access to insights.

How does your organization measure risk?

Responsible data sharing and use requires an assessment of many factors, all of which need to be considered objectively in order to accurately compare data sharing options. Only then can data custodians determine the most appropriate option for their particular circumstances, given the risks and benefits of sharing data in the first place. **Privacy Analytics' approach to risk-based anonymization has been proven to help achieve the balance between protecting individual identity and optimizing data utility[5].**



Example of a risk measurement paradigm by Dr. Khaled El Emam, author, Guide to the De-identification of Health Information (CRC Press, 2013).

With Privacy Analytics, you can safely de-identify and anonymize your data to the highest possible standard—and preserve its utility. By measuring the re-identification risk of personal or protected health information, even your most sensitive data assets can become powerful business drivers.

[5] El Emam, K. and Arbuckle, L., "De-identification and Data Quality" Chapter 13, *Anonymizing Health Data: Case Studies and Methods to Get You Started (O'Reilly Media, 2014)*

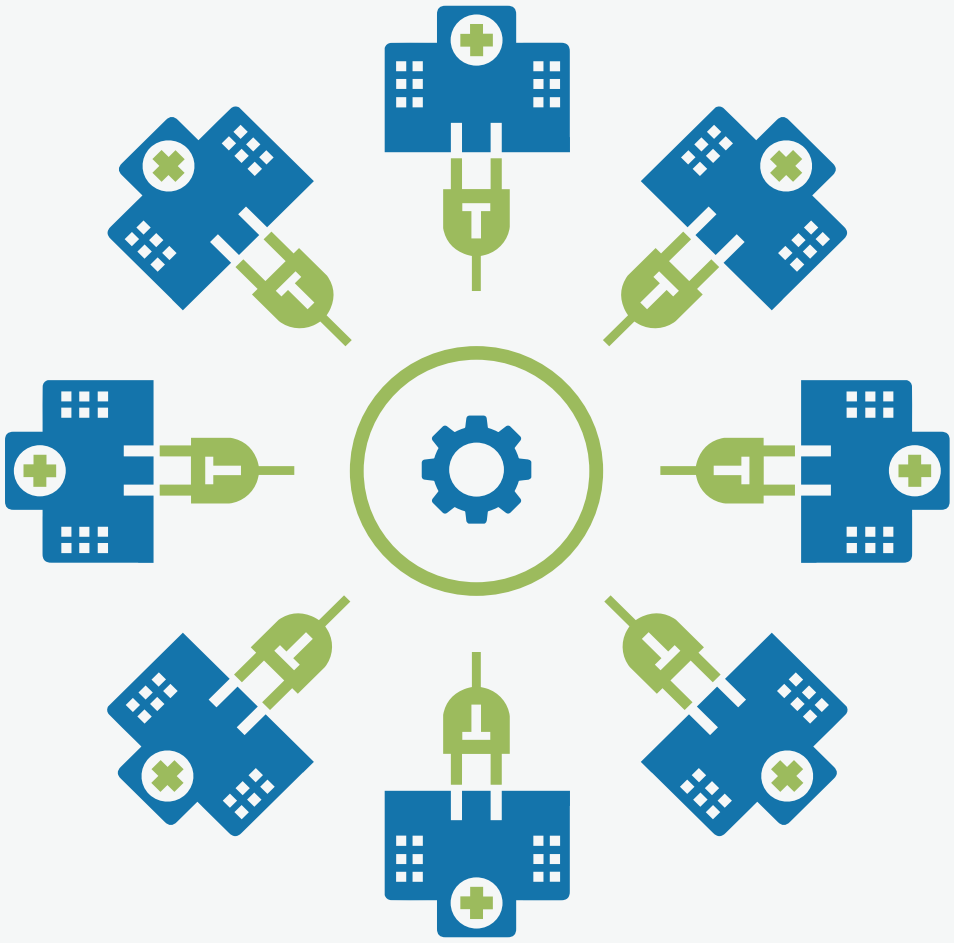
How Privacy Analytics enables innovation, efficiency and competitive advantage in MedTech

Privacy Analytics works with medical device companies to establish an anonymization methodology and integrate secure, repeatable de-identification processes into their data flows. This can make considerations of privacy and ethics far easier to address. As a result, companies can safely use real world data to gain efficiencies and competitive edge in areas such as:

- Researching and developing new products
- Defending marketing / product claims
- Creating and curating data lakes
- Validating product efficiencies
- Metrics regarding medical device consumables
- Precision medicine
- QA testing
- Wearables

AI and Machine Learning are more than just industry buzzwords

A risk-based approach to anonymization can enable artificial intelligence and machine learning initiatives that drive new developments. Using Privacy Analytics data de-identification methodology at source, companies can train models on anonymized data within a safe environment to reduce privacy risks. With this approach, the models look for patterns related to the desired outcome and not from identifiable features. This increases a model's ability to generalize and reduces certain biases towards personal information. Several ethical AI frameworks also feature anonymization as a core element, since using anonymized data instead of identifiable information itself mitigates ethical concerns.



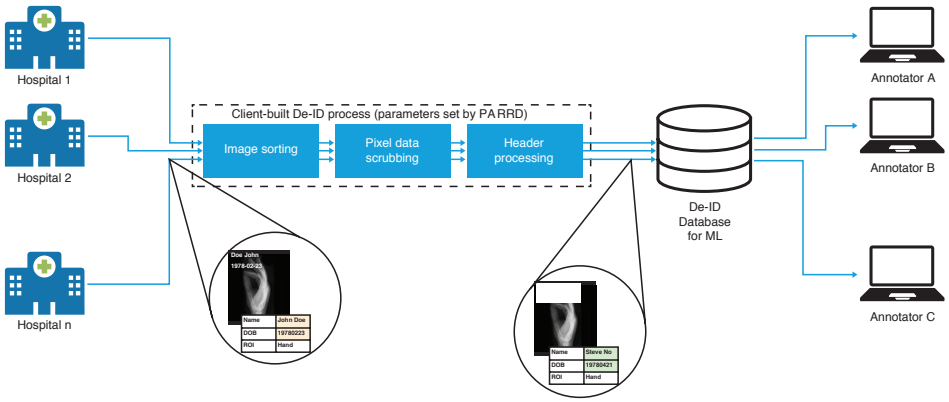
The Hub and Spoke Model: Filling the data lake with safe data from a hub-and-spoke data collection model to enable artificial intelligence and machine learning. Infographic: Luk Arbuckle, Privacy Analytics.

> Working with Privacy Analytics, our clients can precisely assess the quality of their data feeds, leverage the analytics in real time, and achieve internal process improvements.
>
> **Luk Arbuckle, Chief Methodologist, Privacy Analytics, co-author, *Anonymizing Health Data: Case Studies and Methods to Get You Started* (O'Reilly Media, 2014)**

Privacy Analytics enables real world evidence for medical image de-identification

Privacy Analytics has provided services projects on medical image datasets for a variety of medical devices. With more organizations looking to leverage their medical imaging data, Privacy Analytics is packaging our image de-identification services as a standard offering. Our service harnesses the expertise of de-identification professionals to assess the risk of leaks using statistical techniques.

DICOM



Sample of DICOM data automation workflow engineered for a Privacy Analytics client using machine learning for hospital networks. Infographic: Dr. Brian Rasquinha, Privacy Analytics.

Data de-identification to support machine-learning applications

Medical images require special consideration for de-identification to be useful in research for machine learning applications in computer-assisted diagnoses, detailed 3D measurements for biomechanics, sharing fMRI image volumes for psychology or neurology studies, and as documentation of treatment results for surgeries. Privacy Analytics has made significant advances in enabling the secondary use of medical images to drive innovation.

Some of our client success stories:

- For a leader in surgical robotic systems using data from Clinical Case Reports (CCRs), we enabled the client to share high-quality data for secondary purposes while balancing the regulatory requirements and achieving an acceptable risk threshold.
- For a software company using artificial intelligence to derive diagnoses from medical images sourced from a variety of hospital partners and hardware configurations, we enabled the client to apply the process of de-identification to the onboarding of new machines.
- For a global provider of pre-operative planning software and intra-operative surgical robots, we enabled the client to implement privacy and security controls to ensure data recipients can manage data access and use appropriately.

Privacy Analytics' consulting, services and software: the end-to-end, single-source approach to data privacy

Responding to our clients' specific needs, our global team of data scientists and business analysts provide in-depth evaluation of organizations' use cases, data flows, and data assets. Our complete range of solutions includes on-site consulting, assessment, anonymization software and training.

> By adopting responsible data sharing practices, researchers, companies and the general public can gain the benefits and the promise of big data analytics without sacrificing personal privacy or infringing upon law or regulation.
>
> **Dr. Khaled El Emam, CEO, Privacy Analytics, *Risky Business: Sharing Health Data While Protecting Privacy,* Trafford Publishing, 2013**

We invite you to contact us to discuss how your company can gain a competitive advantage.

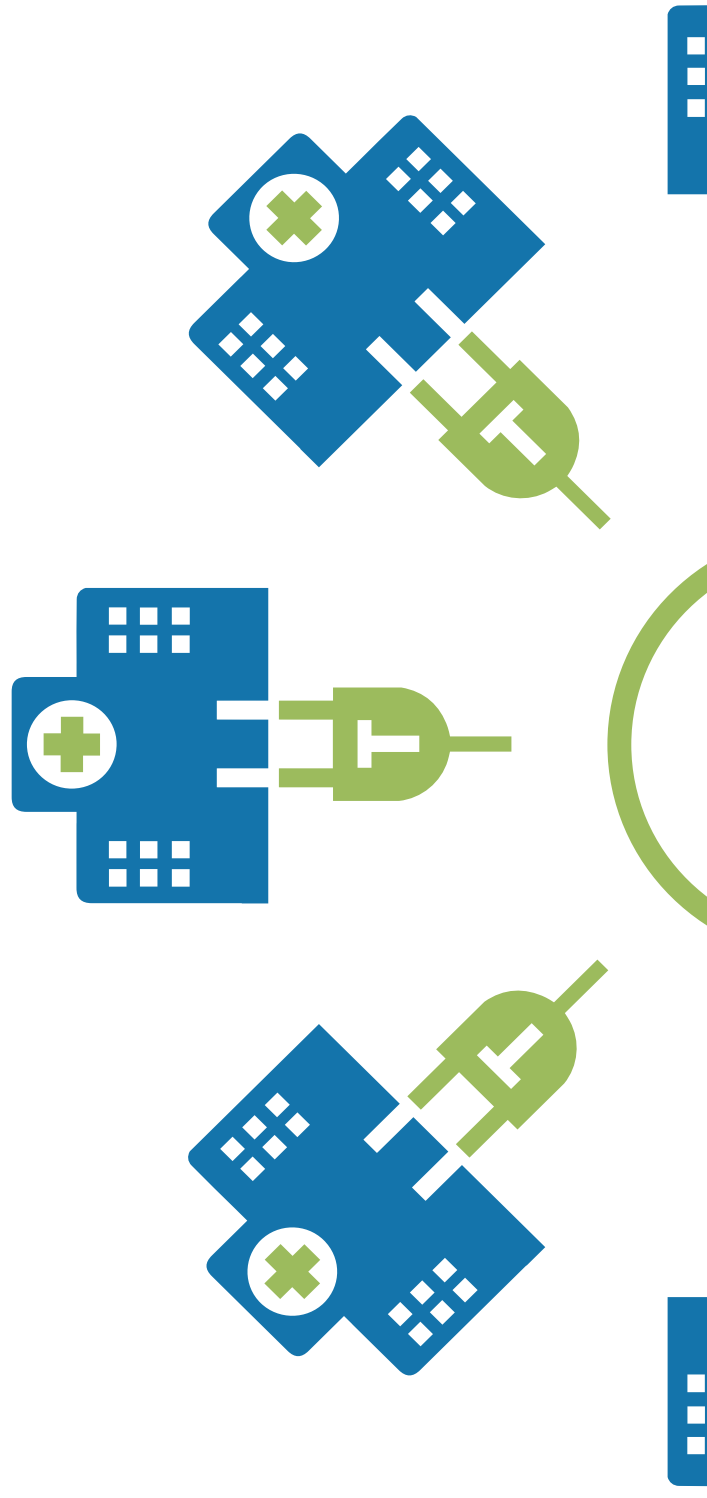
Contact the authors of this position paper:

Khaled El Emam
CEO
kelemam@privacy-analytics.com
linkedin.com/in/kelemam

Luk Arbuckle
Chief Methodologist
larbuckle@privacy-analytics.com
linkedin.com/in/lukarbuckle

To learn more, please visit:

www.privacy-analytics.com



PRIVACY ANALYTICS
an IQVIA company

Privacy Analytics Incorporated

251 Laurier Avenue West, Suite 200
Ottawa, Ontario, Canada K1P 5J6

Telephone: +1 613 369 4313

Toll free: +1 855 686 4781

Fax: +1 613 369 4312

Email: sales@privacy-analytics.com

Visit us on the web: www.privacy-analytics.com

© Copyright 2019, Privacy Analytics Incorporated. All rights reserved.