Medical AI Security and Data Privacy in the Age of Computer Vision

Computer vision – a type of AI that enables computers to generate meaningful information from digital images and take action or make recommendations based on that information – is exploding in the healthcare and life sciences fields.

Because of its ability to foster medical breakthroughs, improve care, make more accurate medical decisions and lower costs, the Global Computer Vision in Healthcare Market is expected to reach $416 billion by 2025 due to the increasing demand to extend the adoption of AI-based technologies.

Annotating Medical Images

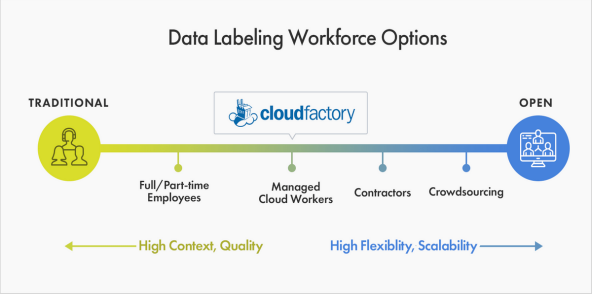
The value of computer vision in healthcare and life sciences is created by the machine learning process of data labeling or data annotation, using training data to show the outcome you want your machine learning model to predict. You are marking, labeling, tagging, transcribing, or processing a dataset with the features you want your machine learning system to learn to recognize.

While computer vision algorithms have made tremendous advances over the past few years, they are not perfect. The challenge for organizations deploying computer vision for medical AI is to increase data labeling and annotation accuracy and quality while controlling costs. The most efficient way to do this is by training a workforce to annotate highly-technical images and videos who understand the nuances of medical processes.

Security Concerns with Managed Workforces or Crowdsourcing Options

Given the healthcare industry isn't immune to the growing skills shortage, organizations needing data labeling expertise are turning to 3rd party options, including crowdsourcing or working with managed workforces specifically trained on medical image and video data annotation.

It's essential to understand who is handling your data. A major concern with crowdsourcing options is you don't always know. This problem can persist at some managed workforce providers who rotate different people in and out of projects on a regular basis.



Either option you choose should have robust data security and business continuity policies in place to ensure safety and consistency when working with medical clients. In addition, a set of core security offerings that cover key aspects of people, process, and technology – from GDPR, SOC2, ISO-9001, and HIPAA/PHI – should be in place.

The cost of not having these policies in place can

quickly escalate. In some cases, violating security and privacy protocols can result in fines of up to $1.5 million per violation – but even greater are the incalculable ethical, moral, and reputational costs of such violations.

Adhering to Medical and Security Standards

When trusting your medical image and video data annotation needs to a third party, there are numerous certifications, regulations, or standards that you will want to understand, and some of these you may consider to be optional, while others you may consider to be requirements. It can highly depend on your and your client's unique data needs and preferences. Some of these include:

ISO 9001 provides a framework and set of principles that ensure a common-sense approach to the management of your organization to satisfy customers and other stakeholders consistently. In simple terms, ISO 9001 certification provides the basis for effective processes and effective people to deliver an effective product or service time after time.

AICPA System and Organization Controls (SOC) is a suite of service offerings CPAs may provide in connection with system-level controls of a service organization or entity-level controls of other organizations. SOC2 is an auditing procedure that ensures your service providers securely manage your data to protect the interests of your organization and the privacy of its clients. For security-conscious businesses, SOC2 compliance is a minimal requirement when considering a SaaS provider.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that requires the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The HIPAA rules and regulations consist of three major components, the HIPAA Privacy rules, Security rules, and Breach Notification rules.

The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas.

Security and Your Data Labeling Workforce

A quality data labeling workforce will prioritize your security concerns so your team can focus on strategic priorities.

Most importantly, your data labeling service must respect data the way you and your organization do. They also should have a documented data security approach in all of these three areas:

- **People and Workforce:** This could include background checks for workers and may require labelers to sign a non-disclosure agreement (NDA) or similar document outlining your data security requirements. The workforce could be managed or measured for compliance. It may include worker training on security protocols related to your data.
- **Technology and Network:** Workers may be required to turn in devices they bring into the workplace, such as a mobile phone or tablet. Download or storage features may be disabled on devices workers use to label data. There's likely to be significantly enhanced network security.
- **Facilities and Workspace:** Workers may sit in a space that blocks others from viewing their work. They may work in a secure location, with badged access that allows only authorized personnel to enter the building or room where data is being labeled. Video monitoring may be used to enhance physical security for the building and the room where work is done.