Top 5 Ways to Protect and Secure Data in the Age of AI

Sucharita Venkatesh
Senior Director General Management, Publicis Sapient, London, United Kingdom

Todd Cherkasky
GVP Customer Experience & Innovation Consulting, Publicis Sapient, Chicago, IL

Francesca Sorrentino
Client Partner, Publicis Sapient, London, United Kingdom

In the rapidly evolving landscape of AI, data protection has become a paramount concern.

Why is AI data security important?

The FTC has made it clear: Model-as-a-service companies must honor their privacy commitments and refrain from using customer data for undisclosed purposes or face serious consequences, including the deletion of unlawfully obtained data and models. For enterprises leveraging AI tools, particularly generative AI built on large language models (LLMs) or extensive internal datasets, the stakes are high. A data breach could expose confidential customer information, leading to significant liability.

But the risk doesn't stop there. Employees or customers may inadvertently input confidential company data or other private information into these

generative AI tools. Without robust safeguards, this data could be exposed, putting the enterprise at risk of legal repercussions and damaging its reputation.

Additionally, in the United States, it is considered unfair or deceptive for a company to adopt more permissive data practices, such as sharing consumer data with third parties or using it for AI training, without clear and upfront communication. Surreptitiously making retroactive amendments to terms of service or privacy policies to inform consumers of such changes can result in severe legal consequences.

However, data and AI are symbiotic and essential to each other's success. AI models rely on vast amounts of data to learn, adapt and improve. Without high-quality, secure data, AI systems cannot function effectively, leading to stunted growth and potential failure. Conversely, AI can enhance data management, providing insights and efficiencies that were previously unattainable.

While some organizations have responded to security risks by banning the use of AI tools, it is crucial to prioritize the security and privacy of data as organizations increasingly rely on AI, particularly generative AI, to foster innovation and enhance efficiency.

What is the biggest issue with AI data protection and security?

Clear policies and guidelines for employees.

According to an Information Systems Audit and Control Association (ISACA) survey, only 10 percent of organizations have a formal, comprehensive generative AI policy in place.

This article explores the top five strategies for your enterprise to protect and secure data when using AI and creating an AI company policy, emphasizing the importance of ethical guidelines, data masking, pseudonymization and transparency.

Protect your business: Get the generative AI risk management playbook

Ensure your organization is equipped to handle the challenges of generative AI. Our **generative AI risk management playbook** provides the insights and tools you need to stay secure. Learn how to fortify your data defenses today.

1. Establish ethical and responsible AI usage guidelines

Before diving into data protection specifics, it's essential to establish comprehensive ethical and responsible AI usage guidelines. These guidelines should address not only data security risks but also other potential risks throughout the AI lifecycle. By setting clear standards, organizations can ensure that their AI initiatives align with ethical AI implementation principles and regulatory requirements.

Key considerations:

- **Ethical AI usage**: Define what constitutes ethical use of AI within your organization
- **Risk management**: Identify and mitigate risks associated with AI, including data privacy, bias and misuse
- **Compliance**: Ensure adherence to relevant data privacy laws and regulations, such as the GDPR and CCPA

2. Avoid using confidential data

One of the most effective ways to safeguard data in generative AI is to avoid using confidential data entirely—either within the LLM training data or as inputs into generative AI tools. By eliminating confidential data from the training and input datasets, organizations can significantly reduce the risk of data breaches and privacy violations.

Why it matters:

- **Minimize risk**: By avoiding the use of confidential data to train the model, organizations can greatly reduce the risk of exposing confidential information
- **Regulatory compliance**: Organizations can avoid the risk of noncompliance with data privacy laws, particularly in the case of personal data, by refraining from using confidential data
- **Customer trust**: Demonstrating a commitment to data privacy builds trust with customers and stakeholders

Practical steps:

- **Data anonymization**: To protect privacy, use anonymized datasets for training AI models
- **Synthetic data**: Generate synthetic data that mimics real data without containing personal data
- **Data minimization**: Collect and use only the data necessary for the specific AI application

Example of when not to use confidential data: In the energy and commodities sector, a generative AI tool designed to predict market trends and prices could avoid using proprietary customer data, such as individual trading strategies, or personal data, such as individual transaction histories, as input or for training the LLM.

Using this sensitive data could lead to competitive disadvantages, breaches of confidentiality agreements and potential regulatory violations. Instead, the AI tool could be trained on aggregated, anonymized market data to ensure

compliance with privacy standards and to protect the proprietary information of individual customers.

3. Implement data masking and pseudonymization

When confidential data is necessary, data masking and pseudonymization are effective techniques to protect it. These methods obfuscate data to help prevent unauthorized access while maintaining its utility for AI applications.

Data masking is a technique used to protect confidential data by modifying it in some way.

Data masking techniques:

- **Replacing names**: Substitute real names with generic identifiers (e.g., "Customer 123")
- **Shuffling data**: Reorder data within a dataset to obscure original values
- **Adding fictitious data**: Modify dates or other sensitive information by a random amount
- **Redaction**: Remove specific fields, such as phone numbers, from datasets to protect privacy

Pseudonymization is a data protection technique that replaces identifiable information within a dataset with pseudonyms or artificial identifiers. Unlike anonymization, which removes all identifying information, pseudonymization allows the data to be reidentified, if necessary, by using a separate key or mapping system.

Pseudonymization techniques:

- **Code replacement**: Replace personal identifiers with unique codes to enhance privacy
- **Hashing**: Convert email addresses or other identifiers into unrecognizable strings

- **Medical record pseudonymization**: Replace patient names with random identifiers while retaining other data for research

4. Balance transparency with confidentiality

Transparency is crucial for building trust in AI systems, but it must be balanced with the need to protect the model's inner workings from misuse. Progressive disclosure, or "detail on demand," is a strategy that allows users to understand AI outputs without revealing too much about the model's internal processes.

How it works:

- **User queries**: When users ask the AI to clarify its answers, the tool highlights relevant input data and cites sources
- **Controlled disclosure**: Provide detailed information only when necessary, ensuring that sensitive aspects of the model remain protected

Example of detail on demand: Consider a generative AI tool used in healthcare for diagnosing diseases based on patient symptoms and medical history. Initially, the AI provides a high-level explanation, such as "Based on the symptoms and medical history, the AI suggests a diagnosis of Disease X." If more information is needed, the healthcare professional can request additional details, like "The AI identified Symptom A and B, common in Disease X, and the patient's history of Condition Y increases the likelihood." This approach maintains transparency, builds trust and protects the model's complex internal workings from potential misuse.

Benefits:

- **Build trust**: To foster user trust, ensure transparency about data sources and AI processes
- **Prevent misuse**: Limit detailed disclosures to help prevent bad actors from exploiting the AI model

5. Partner with robust technology providers

Major technology providers offer advanced data privacy and security solutions that can significantly mitigate data security risks associated with AI. Partnering with these providers can enhance your organization's data protection capabilities.

Cloud storage solutions offered by major technology providers are also designed with advanced security measures to protect sensitive data.

These providers use encryption, both at rest and in transit, to ensure that data is unreadable to unauthorized individuals. They also offer features like multifactor authentication, access controls and data masking services to further enhance data protection.

Storing data in the cloud also allows for real-time monitoring and threat detection. This means that potential security breaches can be identified and addressed promptly, minimizing the risk of data loss or exposure.

Moreover, cloud storage solutions are scalable and flexible, allowing organizations to easily adjust their storage capacity as their data needs change. This is particularly important for AI applications, which often require large amounts of data.

Considerations:

- **Vendor evaluation**: Assess the data privacy and security measures of potential technology partners to mitigate data security risks
- **Security solutions**: Leverage robust security solutions offered by technology providers to protect AI models and data
- **Compliance support**: Ensure that technology partners support compliance with relevant data privacy regulations

Protecting data in the era of AI requires a multifaceted approach that includes ethical guidelines, data avoidance, security controls and balanced transparency. By implementing these strategies, organizations can safeguard

sensitive information, comply with regulatory requirements and build trust with customers and stakeholders.

Top data security, privacy and protection takeaways

- **Rules still apply**: Existing data privacy rules apply to AI, so avoid sneaky data use and begin with ethical guidelines
- **No personal data, no leaks**: Skip personal data in the first iteration of AI tools to avoid privacy headaches, and make sure to keep proprietary algorithms and models within a gated sandbox
- **Protect and secure**: If personal and/or confidential data is a must, add security controls, such as pseudonymization or masking, based on the perceived risk level
- **Transparency with a dose of security**: Let users drill down into AI outputs, revealing data sources without exposing the inner workings of the model. This builds trust and protects your proprietary technology

Taking the first steps toward enterprise AI data security

As AI, and particularly generative AI, continue to evolve, the importance of data protection cannot be overstated. By adopting these top five strategies, organizations can navigate the complexities of AI data security, ensuring that their innovations are both effective and ethical.

Remember, the goal is not only to protect data but also to foster a culture of trust and responsibility in the AI landscape.

Action steps for organizations:

- **Review and update policies**: Regularly reevaluate your AI data privacy policies to ensure they align with the latest AI standards and regulations, as well as general data privacy laws.
- **Educate employees**: Train your team on the importance of data protection and the specific measures your organization is taking.

- **Monitor and audit**: Continuously monitor AI systems for compliance and conduct regular audits to identify and address potential vulnerabilities.
- **Engage stakeholders**: Involve customers, partners and other stakeholders in discussions about data privacy and AI ethics to build a collaborative approach to data protection.

By taking these proactive steps, organizations can harness the power of AI while maintaining the highest standards of data security and privacy.

Publicis Sapient's generative AI solutions

Trust matters. That's why Publicis Sapient's generative AI solutions leverage a deep understanding of data management, ethics, governance and risk to create systems that scale. Grow your business by reducing risk while improving the efficiency of software development and resource allocation.

View our generative AI solutions brochure

Related Topics

Data Privacy & Security | Tech Integration | AI Ethics