Crowe

Checklist

Data Privacy: A Checklist for Life Sciences Companies

Smart decisions. Lasting value.℠

In developing their data integrity program, life sciences companies should consider data privacy concerns through the perspective of data subjects involved in their processes. Patients, research collaborators, clinical trial participants, and other individuals who assist life sciences companies in a myriad of programs expect that their personal data is handled with integrity, fair consideration, and care.

The way in which a company addresses the privacy concerns of data subjects can demonstrate respect, instill a greater sense of trust, strengthen the organization's brand, and encourage more individuals to volunteer to participate in its programs and trials.

Here are some ways life sciences companies can address data subject concerns on the collection, use, retention, and disposal of their personal data.

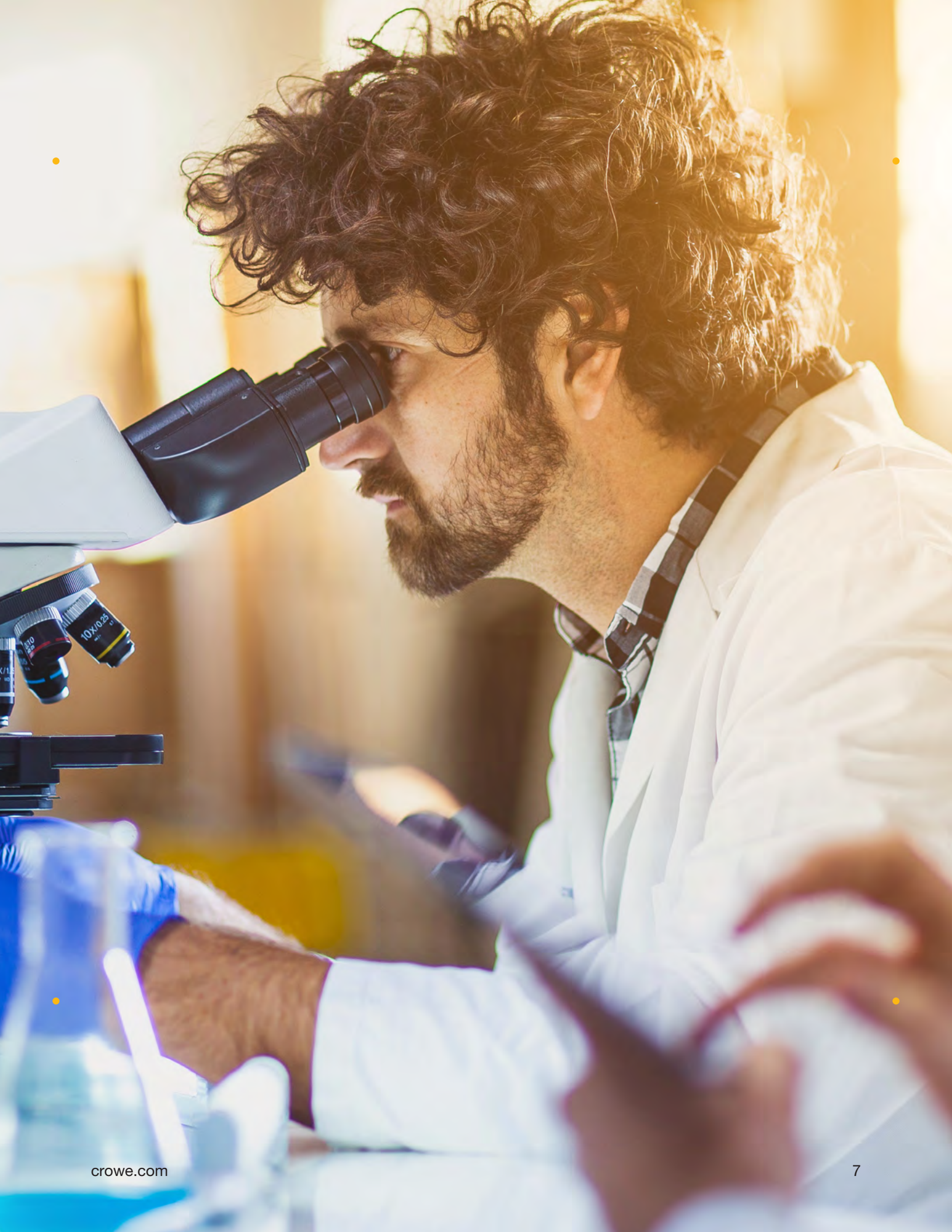
Generally Accepted Privacy Principles (GAPP)

Privacy principles[1]	Data subject privacy concerns	Checklist for maintaining data integrity
Data management	• Does the company have privacy policies and procedures that protect data subjects? • Is someone accountable for protecting personal data? • Are company policies readily available to data subjects for review?	☐ Privacy policies, procedures, and controls are: ◦ Clearly defined ◦ Followed by employees collecting personal data ☐ A corporate privacy officer or other designated person is accountable for implementing, enforcing, and monitoring privacy policies and procedures. ☐ Information about data privacy policies, procedures, and accountability is made available to data subjects.
Privacy notice	• Has the company provided data subjects with a privacy notice that clearly explains its privacy policies and procedures? • Does the privacy notice identify the purposes for which it collects, uses, retains, and discloses personal data? • Have the data subjects been informed of the specific purposes for which their personal data will be used?	☐ The company's privacy notice describes: ◦ What personal data is collected and why collecting personal data is necessary ◦ How it may be used, saved, and securely disposed ◦ Who has access to the personal data, how it is kept safe, and if there is an intention to disclose the personal data to third parties ☐ Changes in the privacy notice are communicated to data subjects in a timely manner. ☐ The privacy notice is written in an understandable format that is easy to comprehend.
Choice and consent	• What options does a data subject have about how personal information is collected, used, and disclosed? • Can the data subject decide to withdraw consent? • Are requests for sensitive data handled with special care?	☐ The privacy notice includes: ◦ Choices available to the data subject regarding the collection, use, and disclosure of personal data ◦ Information about the processes for and consequences of denying or withdrawing consent ☐ Explicit consent is requested for the collection of sensitive data. ☐ Sensitive data is protected with special provisions.

Privacy principles[1]	Data subject privacy concerns	Checklist for maintaining data integrity
Data collection	• How is personal data collected? • Is personal data being collected from third-party sources?	☐ Sources of data and methods of collection are shared with data subjects. ☐ The purpose for the data collection is shared with data subjects. ☐ Processes are defined and used to limit data usage for the expressed purpose. ☐ Due diligence has been conducted with third-party sources to: ◦ Determine if the source is reliable ◦ Confirm that data protection controls and procedures are in place and enforced
Use, retention, and disposal	• What assurance is given that personal data is being used only for the purposes identified? • How long will the company retain personal data? • Will the organization securely dispose of personal data when the original purpose is completed?	☐ Data subjects are informed that their personal data will be used only for the stated purposes identified in the privacy notice. ☐ Systems and procedures are in place to limit the use of personal data to only appropriate and relevant business activities, and in compliance with laws and regulations. ☐ Data subjects are provided information in the privacy notice about: ◦ How long personal data will be retained ◦ How it will be disposed of when the retention period ends
Access to data	• Does the data subject have access to personal data collected for purposes of review and update? • Is there a defined process for the data subject to correct personal data?	☐ The privacy notice provides information on how data subjects can access, review, and update their personal data. ☐ Authentication procedures are enforced that limit access to data subjects. ☐ The process for updating or correcting personal data is defined, communicated, and easily accessible to a data subject.

Privacy principles[1]	Data subject privacy concerns	Checklist for maintaining data integrity
Disclosure to third parties	• Does the company disclose personal data to third parties? • What limits are in place if the data subject chooses to not share personal data with third parties?	☐ The privacy notice: ◦ Describes the reasons, circumstances, and process for disclosing personal information to third parties ◦ Identifies the types and geographic locations of third parties ☐ Controls are in place to prevent the inadvertent or unauthorized disclosure of personal data to third parties. ☐ The organization has and executes a plan to audit third-party compliance regarding use of personal data. ☐ Remedial actions are defined for circumstances in which a third party misuses personal data.
Security for privacy	• How does the company protect personal data from unauthorized access and use? • What safeguards are in place to protect against a data breach? • How does the company notify the data subject if there is a data breach? • What remedies is the company able to provide to data subjects in the event of a data breach?	☐ The privacy notice describes the general security measures and protocols the company has adopted to protect personal data. ☐ The company has established an information security program to protect personal data from loss, theft, misuse, unauthorized access, or destruction. ☐ The company has established processes for identifying incident severity and determining response actions. ☐ The company has procedures for notifying data subjects, when necessary, and complying with breach laws and regulations.

Privacy principles[1]	Data subject privacy concerns	Checklist for maintaining data integrity
Quality	• How does the company maintain the accuracy, completeness, and relevance of personal data for the intended purposes?	☐ The company has established systems and procedures to update personal data while it is retained. ☐ Metadata that describes the data collection (date collected, for example) is recorded. ☐ Processes are in place to ensure personal data collected is still relevant to the purpose for which it is used.
Monitoring and enforcement	• How does the company monitor compliance with its privacy policies and procedures? • How can the data subject register a privacy-related complaint or dispute?	☐ The company's privacy policies address the monitoring and enforcement of privacy policies and procedures. ☐ The corporate privacy officer is authorized to address privacy-related complaints, disputes, and problems. ☐ The company has a formal process in place to handle disputes and provide recourse. ☐ The company annually reviews compliance with its privacy and information security policies and procedures.


10X/0.25

Learn more

To learn more about data privacy and how Crowe can help, contact:

Pam Hrubey
Managing Director
+1 317 208 1904
pam.hrubey@crowe.com

Mindy Herman
Principal
+1 317 706 2614
mindy.herman@crowe.com

---

[1] Generally Accepted Privacy Principles, American Institute of CPAs and the Canadian Institute of Chartered Accountants, August 2009. The 10 GAPP principles are defined by the cited publication and are not industry-specific, but the checklist items in this article represent Crowe analysis of the most critical GAPP considerations for life sciences companies.

crowe.com

MD-19001-045A