

Nano Project: Privacy, Governance and Security Regulations

You were contacted as a data governance and privacy specialist; using the governance principles taught in class, develop a data governance roadmap for your organisation, outlining specific data roles and other key elements of a data management strategy.

Organisation Example: Pharmaceutical Company

1. Comprehensive Assessment:

- The data governance team should conduct a thorough review of the pharmaceutical past and present data management practices by analysing data sources, data integration processes, data storage, data usage across all departments including but not exclusive to the R&D team, clinical trials, manufacturing, and marketing.
- By analysing the data this should identify data related issues such as data silos (isolated data not shared across all departments e.g., master records usually held by quality assurance), inconsistent data definitions due to lack of standardisation and data security vulnerabilities.

2. Identification of Key Stakeholders:

- Key stakeholders can be identified as the Chief Executive Officer (CEO), Chief Data Officer (CDO), Chief Information Officer (CIO), Chief Financial Officer (CFO) Heads of Departments for the following R&D, Regulatory Affairs, Quality Assurance, data owners for each critical data domain (e.g., clinical trial data, adverse event data), data scientists, clinical researchers, IT personnel responsible for data infrastructure, and representatives from legal and compliance teams.

3. Scope:

- The scope is to cover all aspects of data management and data usage within the pharmaceutical company, including research, drug development, clinical trials, manufacturing, marketing, and post-marketing surveillance.
- To establish a robust and efficient data governance framework that ensures data integrity, enhances data-driven decision-making, and enables compliance with industry regulations and to define clear objectives.

4. Objectives:

- Improve data quality and consistency to support accurate and reliable insights in drug development, clinical trials, and manufacturing processes.
- Enhance data security and access controls to protect sensitive patient information and intellectual property.
- Ensure compliance with relevant data privacy regulations (e.g., GDPR, HIPAA) and industry standards (e.g., GxP).
- Facilitate collaboration and data sharing across different departments, promoting cross-functional data insights and knowledge sharing.
- Establish clear roles, responsibilities, and accountability for data management and governance.
- Measure KPI's and report data governance performance to monitor progress and identify areas for improvement.
- Foster a data-driven culture through training and awareness programs for employees at all levels.

5. Data Governance Committee:

- Establish a Data Governance Committee consisting of senior executives, regulatory experts, IT representatives, and data stakeholders from different functional areas (R&D, manufacturing, clinical, regulatory affairs, etc.).
- The committee will oversee and make decisions on data policies, standards, and initiatives related to drug development, production, and regulatory compliance.
- Ensure that the committee has executive sponsorship and buy-in from key stakeholders e.g., The Data Governance Committee consists of representatives from Research & Development, Clinical Trials, Regulatory Affairs, Quality Assurance, IT, and the Chief Data Officer (CDO). They meet bi-monthly to review data governance initiatives, prioritize data-related projects, and make decisions regarding data policies and standards.

5. Establish a Data Governance Framework:

- Create a formal data governance framework that aligns with industry-specific regulations and standards (e.g., MHRA, FDA, EMA, GxP and ISO).
- Define the governance principles, policies, and standards that will govern data management across the organization.
- The framework outlines the structure, policies, processes, and procedures for governing data within the organization. It addresses areas such as data management, data quality, data privacy, data security, and data sharing. The framework should align with the organization's goals, regulatory requirements, and industry best practices. It is developed collaboratively with the involvement of the Data Governance Committee, stakeholders, and subject matter experts.

6. Data Governance Policies and Standards:

- Research and develop comprehensive data governance policies and standards that cover data validation, data retention, data access controls, and audit trails.
- Ensure alignment with industry-specific regulations and best practices e.g., GXP/GDPR/ISO.
- The pharmaceutical company should develop policies and standards covering data classification, data retention, data sharing, and data privacy. For instance, the policy may require that all patient data collected during clinical trials should be stored and transmitted in compliance with GxP regulations and that access to sensitive data is restricted based on role-based access controls.

7. Data Catalogue and Inventory:

- Implement a centralized data catalogue specifically tailored to pharmaceutical data assets.
- Include critical metadata such as drug names, trial IDs, manufacturing batch numbers, manufacturing data, expiry dates, and data lineage information.
- Create an inventory of all data assets, including databases, applications, spreadsheets, and data repositories.
- Classify data based on its sensitivity, criticality, and regulatory requirements.
- For example, establishment of a centralized data catalogue that includes information about clinical trial data, drug development data, adverse events data, manufacturing data, and more. The inventory provides details about data sources, data ownership, data lineage, and data usage.

8. Data Quality Management:

- Establish data quality monitoring processes and metrics for critical data elements.
- Implement data cleansing and enrichment procedures to meet regulatory requirements.
- Establish data quality metrics and procedures to monitor and improve the accuracy, completeness, and reliability of data.
- Implement data profiling and data cleansing activities where necessary.
- Data quality management processes are implemented to assess data accuracy, completeness, and consistency. Data quality metrics are defined to measure the percentage of accurate clinical trial data, identify data errors, and track improvement over time.

9. Data Security, Access Control and Privacy:

- Implement robust data security measures to safeguard sensitive research data, intellectual property, and patient information.
- The company should implement role-based access controls (RBAC) to restrict data access based on user roles and responsibilities. Access permissions are defined and granted to individuals or groups based on their job functions and the data they need to perform their duties.
- For example, a researcher in the R&D department will have access to research data, while a clinical trial coordinator will have access to patient data only for their assigned trials.
- Develop and implement data security measures to protect sensitive and confidential data from unauthorized access or breaches.
- Ensure compliance with data privacy regulations and implement necessary safeguards for data protection such as encryption of sensitive data, two-factor authentication for access to critical systems, and regular security audits to protect patient information and prevent unauthorized access.
- Conduct regular data privacy risk/impact assessments and audits.

10. Data Sharing Agreements:

- The company should establish data sharing agreements with external partners, such as contract research organizations (CROs). These agreements outline the terms, conditions, and restrictions for sharing data, ensuring compliance with data privacy regulations and protecting intellectual property.

11. Data Sharing Platforms and Technologies:

- The company should utilize secure data sharing platforms or technologies that enable controlled sharing of data within and outside the organization. These platforms ensure data integrity, enforce access controls, and provide audit trails for data sharing activities.
- Example: The company implements a secure cloud-based collaboration platform where authorized users can securely share and collaborate on research data, while ensuring that access controls and encryption measures are in place.

12. Data Sharing Protocols and Standards:

- The company establishes protocols and standards for data sharing, including data formats, data exchange protocols, and data anonymization techniques, where applicable. These protocols ensure consistency, interoperability, and privacy protection when sharing data with external stakeholders.
- Example: The company adopts the Clinical Data Interchange Standards Consortium (CDISC) standards for sharing clinical trial data, ensuring data consistency and interoperability with regulatory authorities.

13. Data Sharing Governance and Oversight:

- The Data Governance Committee will oversee data sharing activities, ensuring compliance with data governance policies and applicable regulations. They will review and approve data sharing requests, assess data privacy risks, and provide guidance on secure data sharing practices.
- They should evaluate the data privacy risks associated with sharing sensitive patient data and ensure that appropriate measures are in place to protect the privacy and confidentiality of the data.

14. Data Governance Metrics and Reporting:

- Define key performance indicators (KPIs) to measure the effectiveness of data governance efforts in ensuring regulatory compliance and data quality.
- Establish regular reporting mechanisms to communicate progress and challenges to stakeholders and regulatory bodies.
- Key performance indicators (KPIs) should be established to monitor the effectiveness of data governance initiatives. Metrics like data quality scores, data access audit logs, and data privacy compliance rates are regularly reported to the Data Governance Committee and executive leadership.

15. Continuous Improvement:

- Develop a process for continuous improvement of data governance practices, considering feedback from audits, inspections, and emerging industry trends.
- Continuously review and refine the data governance framework based on feedback, industry best practices, and changing business requirements.

16. Data Training and Awareness:

- Provide specialized training for employees handling pharmaceutical data, emphasizing the importance of data security, privacy, and regulatory compliance.
- Raise awareness and conduct data governance training sessions for employees, emphasizing the importance of data management, security, and compliance.

17. Data Governance Maturity Model:

- Develop a maturity model specific to the pharmaceutical industry to assess the organization's data governance capabilities and drive improvements.
- A data governance maturity model should be developed, with different levels (e.g., ad-hoc, defined, managed, optimized) representing the organization's data governance capabilities. The company assesses its current maturity level and sets targets for progressing to higher levels.

18. Data Governance Communication Plan:

- Develop a communication plan that includes regular updates to employees and stakeholders on data governance initiatives and compliance measures, data governance activities, achievements, and challenges.
- Communications can be presented as Internal newsletters, town hall meetings, and intranet portals are used to keep employees informed. External communications are also established to assure partners, customers, and regulatory bodies about the company's commitment to data governance and compliance.

References:

- GXP' Data Integrity Guidance and Definitions - [letter \(publishing.service.gov.uk\)](https://www.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/614442/gxp-data-integrity-guidance-and-definitions.pdf)
- The Government Data Quality Framework: guidance - <https://www.gov.uk/government/publications/the-government-data-quality-framework/the-government-data-quality-framework-guidance>