Internship Task 4 – Big Data Security and Compliance

Name: Pandya Naiya

Internship Organization: Codetech

Task Title: Task 4 – Big Data Security and Compliance

# Introduction

In today’s digital world, big data is collected and stored at a large scale. This data may include sensitive information such as customer details, medical records, financial data, etc. Therefore, it is important to protect this data by applying proper security measures and following compliance regulations.

# What is Security and Compliance in Big Data?

Security refers to the protection of data from unauthorized access, theft, or misuse.  
Compliance means following certain rules and regulations like:  
- GDPR (General Data Protection Regulation) – Protects personal data of EU citizens.  
- HIPAA (Health Insurance Portability and Accountability Act) – Protects health-related information.  
Organizations must follow these regulations to avoid legal issues and build trust with users.

# Framework for Big Data Security and Compliance

|  |  |
| --- | --- |
| Component | Description |
| Data Classification | Identify and label data as sensitive or non-sensitive. |
| Access Control | Only authorized users should access certain data (via roles or permissions). |
| Encryption | Encrypt data at rest and during transmission to prevent misuse. |
| Consent Management | Always take user consent before collecting personal data. |
| Audit & Logging | Maintain logs of who accessed what data and when. |
| Data Masking | Hide sensitive parts of data for unauthorized viewers. |
| Data Retention Policy | Keep data only for the required time period. |
| Compliance Check | Regular audits to ensure GDPR, HIPAA rules are followed. |

# Real-Life Example

Suppose a hospital uses a big data system to manage patient records.  
Using this framework:  
- Patient data is encrypted.  
- Only doctors with access rights can view records.  
- Every access is logged.  
- Consent is taken before storing any patient detail.  
This ensures privacy and legal compliance.

# Conclusion

Big Data Security and Compliance is essential for any organization that deals with large amounts of personal or sensitive data. By implementing a proper framework, organizations can protect user data, gain user trust, and avoid legal risks.

# Table of Compliance Standards

|  |  |  |
| --- | --- | --- |
| Standard | Purpose | Used In |
| GDPR | Protect user personal data (EU) | Websites, CRMs |
| HIPAA | Protect medical/health information | Hospitals, Clinics |
| CCPA | Data privacy law for California residents | eCommerce, Apps |