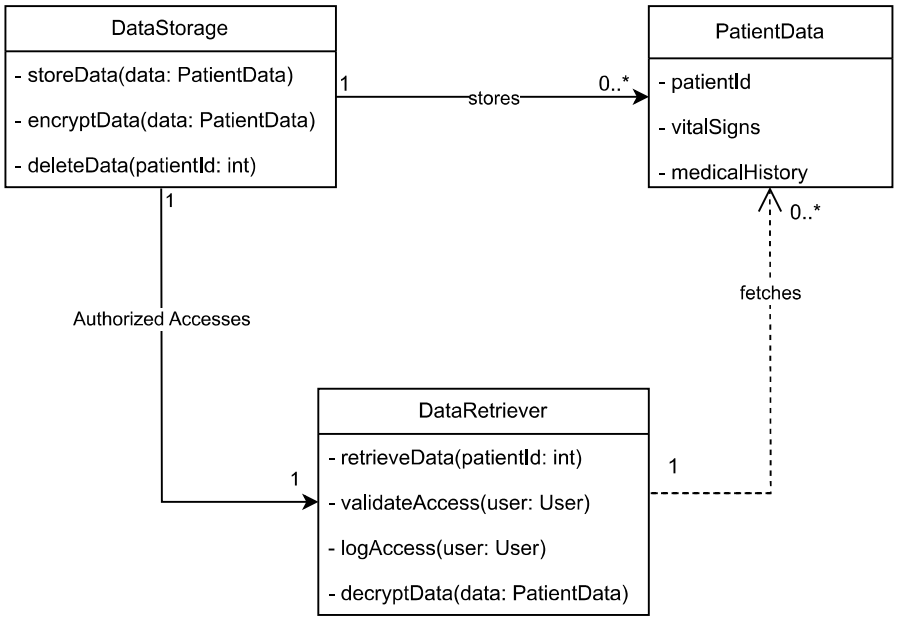

The UML diagram for the Data Storage System is designed to encapsulate the interactions and responsibilities involved in handling sensitive patient data within a healthcare system. The primary class, DataStorage, is responsible for the core functionalities of storing, encrypting, and deleting patient data. These operations ensure that patient data is not only preserved but also protected from unauthorized access, and obsolete data can be removed in compliance with data protection regulations.

The PatientData class serves as a container for patient-specific information, such as identification, vital signs, and medical history. The relationship between DataStorage and PatientData is defined as a one-to-many association, where a single instance of DataStorage manages multiple instances of PatientData. This design choice reflects the real-world necessity of a centralized storage system capable of handling data from multiple patients.

The DataRetriever class is tasked with fetching patient data. It includes methods for retrieving data, validating access permissions, logging access for audit purposes, and decrypting data for use. The multiplicity between DataRetriever and PatientData indicates that one instance of DataRetriever can interact with many pieces of patient data, supporting the functionality for batch processing or queries across multiple records.

This UML diagram emphasizes security and efficient data management, aligning with healthcare industry standards for data integrity and confidentiality. The choice to explicitly model encryption and decryption processes within the DataStorage and DataRetriever classes respectively, underscores the critical importance of data security in medical applications. The overall architecture aims to provide a robust framework for secure data handling, ensuring that data is accessible only to authorized personnel and that all access is traceable and secure.