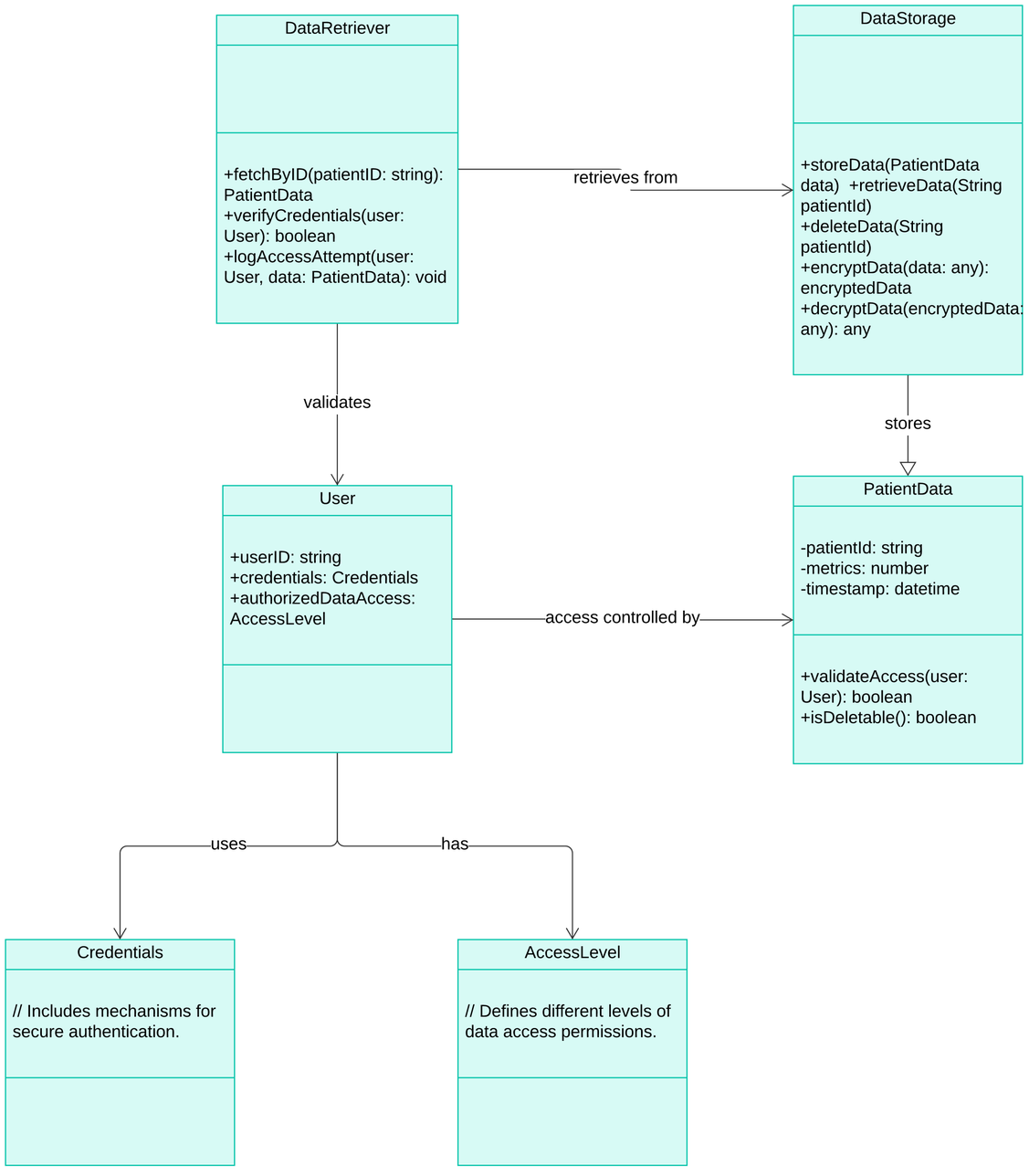

1. **DataRetriever**: This class is tasked with fetching patient data and verifying user credentials, acting as an intermediary between User and DataStorage. The "retrieves from" arrow shows that DataRetriever pulls information from DataStorage, while the "validates" arrow to User represents the checking of credentials.
2. **DataStorage**: It interacts directly with PatientData, storing and managing it. It offers functionality for encryption and decryption, highlighting the system's emphasis on data security. The "retrieves from" arrow indicates that data flows from DataStorage to DataRetriever after a successful retrieval operation.
3. **PatientData**: As the central data class, it holds patient-specific health information, including an ID, health metrics, and a timestamp. The arrows pointing towards it represent data storage and access validation operations.
4. **User**: This class embodies the end-user with specific properties like ID and credentials, along with an AccessLevel that dictates what data they can access. The "access controlled by" arrow denotes that PatientData access is determined by the User's AccessLevel.
5. **Credentials**: This class is used by User and encapsulates authentication mechanisms, as indicated by the "uses" association. This separation underlines the modular approach to security, allowing for different authentication methods to be employed without altering the User class structure.
6. **AccessLevel**: Linked to User, it defines the permissions granted to the user, determining which operations on PatientData they're allowed to perform.

User's access to PatientData through DataRetriever ensures that only authenticated and authorized actions are performed, safeguarding patient information. The diagram has a robust authorization mechanism, which is essential for compliance with healthcare data protection regulations.