**CETM75 Assignment 1: Database Design**

**School of Computer Science**

**University of Sunderland**

Table of Contents

[Task 1: Smith and Co Second-Hand Bookshop 1](#_Toc146199738)

[Task 2: St. John’s Hospital 4](#_Toc146199739)

# Task 1: Smith and Co Second-Hand Bookshop

**Scenario:**

The Smith and Co second-hand bookshop wishes to maintain data on their customers, authors and books. They may have many books by each author in the bookshop at one time. Books may be bought and sold several times. In other words, as the bookshop is a second-hand store they may sell a book, then buy it back off the customer at a later date to sell on to another customer.

**Normalisation Table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Unnormalized | UNF Level | 1NF | 2NF | 3NF |
| Customer Id  Name  Email  Address 1  Address 2  Address 3  Postcode  Author Id  Author Name  Book Title  Purchase Date  Sales Price | 1  1  1  1  1  1  1  2  2  1  1  1 | Customer Id  Name  Email  Address1  Address2  Address3  Postcode  Purchase Id  \*Customer Id  Author Id  BookId  Author Name  Book Title  Purchase Date  Sales Price | Customer Id  Name  Email  Address 1  Address 2  Address 3  Postcode  Author Id  Author Name  BookId  \*Author Id  Book Title  Purchase Id  \*BookId  \*Author Id  \*Customer Id  Purchase Date  Sales Price | Customer Id  Name  Email  Address 1  Address 2  Address 3  Postcode  Author Id  Author Name  BookId  \*Author Id  Book Name  Purchase Id  \*Author Id  \*BookId  \*Customer Id  Purchase Date  Sales Price |

**\* represent foreign key**

**\_ represent primary key**

In 2NF, each non-key attribute is fully dependent on the primary key, and there are no partial dependencies and also there are no transitive dependencies in the 2NF tables therefore 3NF is same as 2NF.

**Write a report (of approximately 500 words) on any two potential database**

**Attacks which could occur on the Smith and Co Second-Hand bookshop database. For each attack:**

* **Include information relating to why the database might be a target for an attack.**
* **The type of attacks which may occur.**
* **The type of data that might be extracted from the system in each attack.**

The smith and co Second-Hand Bookshop’s database contains sensitive customer’s data and transactional data, making it an attractive spot for malicious hackers. Here I have discussed two major database attacks that could target the bookshop database.

**1: SQL Injection Attack**

Starting with why this database might be a target for this type attack as this database holds valuable customers information including name, emails, address and purchase details. Attackers might try to exploit vulnerabilities to access, manipulate or steal this data for various malicious purpose such as identity theft or fraud. In this type of attack SQL injection is a common attack vector where an attacker injects malicious SQL queries into input fields, aiming to manipulate the database SQL statements. If the database does not properly sanitize and validate user input, attackers can execute arbitrary SQL commands.

This type of attack on Bookshop database can lead to loss of sensitive information including customer names, emails, purchase history and potentially data of financial transaction if it’s present in the database. Attacker might also gain unauthorized access to the database management system, enabling further exploitation.

**Prevention and Mitigation:**

Input validation: Implement rigorous input validation and sanitization to remove potentially malicious SQL queries from uses inputs.

Prepared Statements: Use prepared statements and parameterized queries to separate user inputs from SQL statements.

Web App. Firewall (WAF): use a WAF to filter and block SQL injection attempts.

**2: Data Breach via unauthorized access**

The bookshop database contains valuable customer data and purchase records. Unauthorized access to this data can lead to identify theft, financial frauds and most importantly privacy violations. Moreover the database may also store credit card details in future, making it attractive to attackers seeking financial data for fraudulent purpose. This type of attack involves exploiting vulnerabilities in the system authentication and access control mechanism to gain unauthorized access to the database. In this type of attack, attackers could potentially extract a wide range of sensitive data, including customers name, email, address, postal address and even finance related data. This data can be used for various malicious purpose such as phishing, spamming, or identity theft.

**Prevention and Mitigation:**

Strong Authentication: Implement strong authentication mechanisms, including two-factor authentication, to verify user identities.

Access Control: Enforce strict access control policies and permissions to limit database access to authorized users and roles.

Encryption: Encrypt sensitive data at rest and in transit to protect it from unauthorized access.

Logging and Monitoring: Implement robust logging and monitoring solutions to detect and respond to suspicious activities.

Regular Auditing: Conduct regular security audits and vulnerability assessments to identify and remediate security weaknesses.

**References:**

* *https://owasp.org/www-community/attacks/SQL\_Injection*.
* Force, J.T. (2020) *Security and Privacy Controls for Information Systems and Organizations*, *CSRC*. Available at: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (Accessed: 19 September 2023).

# 

# Task 2: St. John’s Hospital

Produce an E-R diagram and data dictionary for the following scenario. Ensure you think carefully about entity names and attribute names and data types.

**Scenario:**

Introduction

St John’s hospital are updating their filing systems and want to move their medical records within their hospital pharmacy to a computerised system to enable ease of use for staff and to modernise their old paper-based filing system. You have been tasked with developing a database application to meet their needs.

**These are the assumptions I have taken for creating this ER diagram:**

* Each patient can have multiple prescriptions.
* Each prescription can only be for one drug.
* Each prescription can only be dispensed once.
* Each prescription can only be associated with one doctor.
* Each prescription can only be dispensed by one pharmacist.

**Labelled Relationships:**

* Patient - Prescription (Has)
* Prescription - Drug (Is For)
* Prescription - Doctor (Written By)
* Prescription - Pharmacist (Dispensed By)

**Cardinality Constraints:**

* Patient : Prescription 1 : M
* Prescription : Drug 1 : 1
* Prescription : Doctor 1 : 1
* Prescription : Pharmacist 1 : 1
* Prescription : Prescription Details 1 : 1

**Entity-Relationship Diagram:**

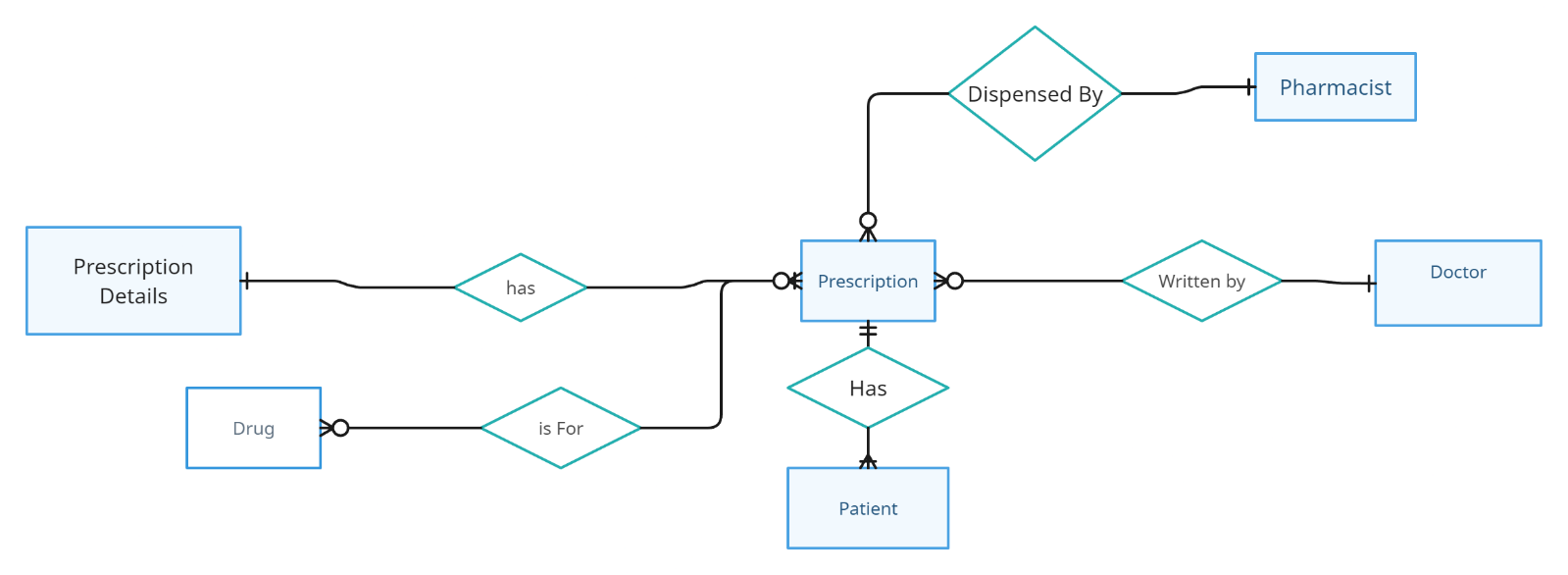


Figure 1 : ER Diagram

**Data Dictionary for St. John Hospital Database**

**For Patience Table**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Attribute** | **Data Type** | **Length** | **Required** | **Validation** | **Format** | **PK** | **FK** | **Comments** |
| **Patient id** | serial |  | Y |  |  | Y |  |  |
| name | VARCHAR |  | Y |  |  |  |  |  |
| Address | VARCHAR |  |  |  |  |  |  |  |
| DOB | DATE | DDMMYY | Y |  |  |  |  |  |
| telephone | numeric |  | Y |  |  |  |  |  |

**For Drug Table**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Attribute** | **Data Type** | **Length** | **Required** | **Validation** | **Format** | **PK** | **FK** | **Comments** |
| **Drug id** | serial |  | Y |  |  | Y |  |  |
| name | VARCHAR |  | Y |  |  |  |  |  |
| Cost | numeric |  | Y |  | 99.99 |  |  |  |
| Stock | INT |  | Y |  |  |  |  |  |

**For Doctor Table**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Attribute** | **Data Type** | **Length** | **Required** | **Validation** | **Format** | **PK** | **FK** | **Comments** |
| **Doctor id** | serial |  | Y |  |  | Y |  |  |
| name | VARCHAR |  | Y |  |  |  |  |  |

**For Pharmacist** **Table**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Attribute** | **Data Type** | **Length** | **Required** | **Validation** | **Format** | **PK** | **FK** | **Comments** |
| **Pharmacist id** | serial |  | Y |  |  | Y |  |  |
| name | VARCHAR |  | Y |  |  |  |  | NOT NULL |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Attribute** | **Data Type** | **Length** | **Required** | **Validation** | **Format** | **PK** | **FK** | **Comments** |
| **Prescription id** | serial |  | Y |  |  | Y |  |  |
| **Patient id** | INTEGER |  | Y |  |  |  | Y |  |
| **Doctor id** | INTEGER |  | Y |  | 99.99 |  | Y |  |
| **Pharmacist id** | INTEGER |  | Y |  |  |  | Y |  |
| **Issue date** | DATE |  |  |  |  |  |  | NOT NULL |
| **Quantity issued** | INTEGER |  |  |  |  |  |  | NOT NULL |

**For Prescription Table**

**For Prescription Details Table**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Attribute** | **Data Type** | **Length** | **Required** | **Validation** | **Format** | **PK** | **FK** | **Comments** |
| **Prescription Details id** | Serial |  | **Y** |  |  | Y |  |  |
| **Prescription id** | INTEGER |  | Y |  |  |  | Y |  |
| **Patient id** | INTEGER |  | Y |  |  |  | Y |  |
| **Doctor id** | INTEGER |  | Y |  | 99.99 |  | Y |  |
| **Pharmacist id** | INTEGER |  | Y |  |  |  | Y |  |
| **Prescribed date** | DATE |  |  |  |  |  |  | NOT NULL |
| **Quantity**  **Prescribed** | INTEGER |  |  |  |  |  |  | NOT NULL |