4.13: SA1 - Database Design

Mina R.R. Ghabrial (239758130)

University of Sunderland

CETM75 - Secure Database Systems

Randa Almadhoun

November 23, 2024

Table of Contents

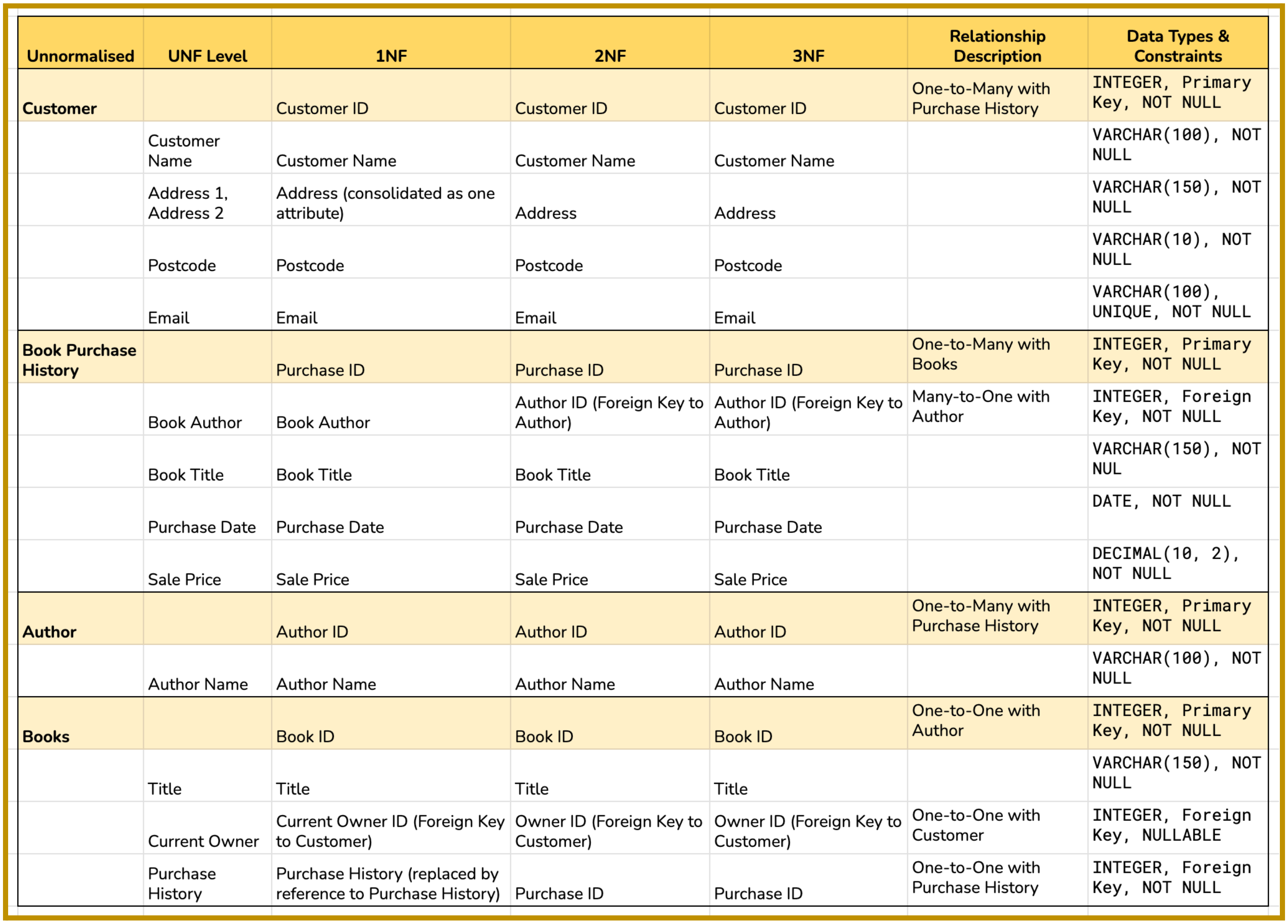
Task 1: Smith and Co Second-Hand Bookshop

Normalisation Table

This normalisation table details entities, attributes, and relationships up to Third Normal Form (3NF). Primary and foreign key roles are explicitly indicated to highlight the integrity and relationships between entities, such as "Customer ID" linking customers to their respective purchase histories and "Author ID" linking books to their authors. Key attributes have been noted for their role within the data model:

- Email is used for customer notifications and marketing purposes.
- Purchase Date records the specific date a book was purchased, providing transactional history.

The relationships are described with clear cardinality, such as one-to-many between Customers and Book Purchase History, to ensure that all dependencies and data flows are well understood.



Unnormalised	UNF Level	1NF	2NF	3NF	Relationship Description	Data Types & Constraints
Customer		Customer ID	Customer ID	Customer ID	One-to-Many with Purchase History	`INTEGER, Primary Key, NOT NULL`
	Customer Name	Customer Name	Customer Name	Customer Name		`VARCHAR(100), NOT NULL`
	Address 1, Address 2	Address (consolidated as one attribute)	Address	Address		`VARCHAR(150), NOT NULL`
	Postcode	Postcode	Postcode	Postcode		`VARCHAR(10), NOT NULL`
	Email	Email	Email	Email		`VARCHAR(100), UNIQUE, NOT NULL`
Book Purchase History		Purchase ID	Purchase ID	Purchase ID	One-to-Many with Books	`INTEGER, Primary Key, NOT NULL`
	Book Author	Book Author	Author ID (Foreign Key to Author)	Author ID (Foreign Key to Author)	Many-to-One with Author	`INTEGER, Foreign Key, NOT NULL`
	Book Title	Book Title	Book Title	Book Title		`VARCHAR(150), NOT NUL`
	Purchase Date	Purchase Date	Purchase Date	Purchase Date		`DATE, NOT NULL`
	Sale Price	Sale Price	Sale Price	Sale Price		`DECIMAL(10, 2), NOT NULL`
Author		Author ID	Author ID	Author ID	One-to-Many with Purchase History	`INTEGER, Primary Key, NOT NULL`
	Author Name	Author Name	Author Name	Author Name		`VARCHAR(100), NOT NULL`
Books		Book ID	Book ID	Book ID	One-to-One with Author	`INTEGER, Primary Key, NOT NULL`
	Title	Title	Title	Title		`VARCHAR(150), NOT NULL`
	Current Owner	Current Owner ID (Foreign Key to Customer)	Owner ID (Foreign Key to Customer)	Owner ID (Foreign Key to Customer)	One-to-One with Customer	`INTEGER, Foreign Key, NULLABLE`
	Purchase History	Purchase History (replaced by reference to Purchase History)	Purchase ID	Purchase ID	One-to-One with Purchase History	`INTEGER, Foreign Key, NOT NULL`

Short Report

The Smith and Co second-hand bookshop database stores sensitive information such as customer details, book inventory, and transaction history, making it an attractive target for attackers. Small businesses like Smith and Co are particularly vulnerable due to limited security resources. This report will discuss two potential attacks on the bookshop's database: SQL Injection and Phishing with Credential Harvesting.

Why the Smith and Co Database is a Target for Attacks

The Smith and Co bookshop database is an appealing target for cybercriminals for several reasons. Firstly, the database contains a wealth of personal information, such as customer names, email addresses, and purchase histories, all of which can be used for identity theft or further targeted attacks. This personal data is valuable, both on the dark web and for malicious actors who wish to exploit it directly.

In addition to customer data, the bookshop also maintains transactional records, including purchase prices and dates, which provide insight into the bookshop's operations and finances. Furthermore, operational data such as stock levels and book inventory details can be of interest to competitors or could be used for sabotage, affecting the business's supply chain and operations.

Given the sensitive nature of the data and the fact that Smith and Co is a small business with likely limited security measures, attackers view it as a relatively easy opportunity for data extraction and manipulation. Without strong defences, the database is vulnerable to attacks that could compromise its confidentiality, integrity, and availability.

SQL Injection Attack

SQL Injection is a common database attack that targets input fields, like search bars or login forms, by injecting malicious SQL commands. When inputs are not properly sanitised, these commands execute directly, allowing attackers to bypass security, access, and manipulate the database. For Smith and Co, SQL Injection could lead to unauthorised access to customer data, such as names, addresses, and transaction histories, potentially resulting in identity theft or fraud. Attackers could also alter or delete inventory records, disrupting daily operations. To prevent this, Smith and Co should implement input validation and parameterised queries for all database interactions (OWASP, 2023). Following NIST guidelines on secure coding practices and regular database audits can further mitigate these risks (NIST, 2023).

Phishing and Credential Harvesting

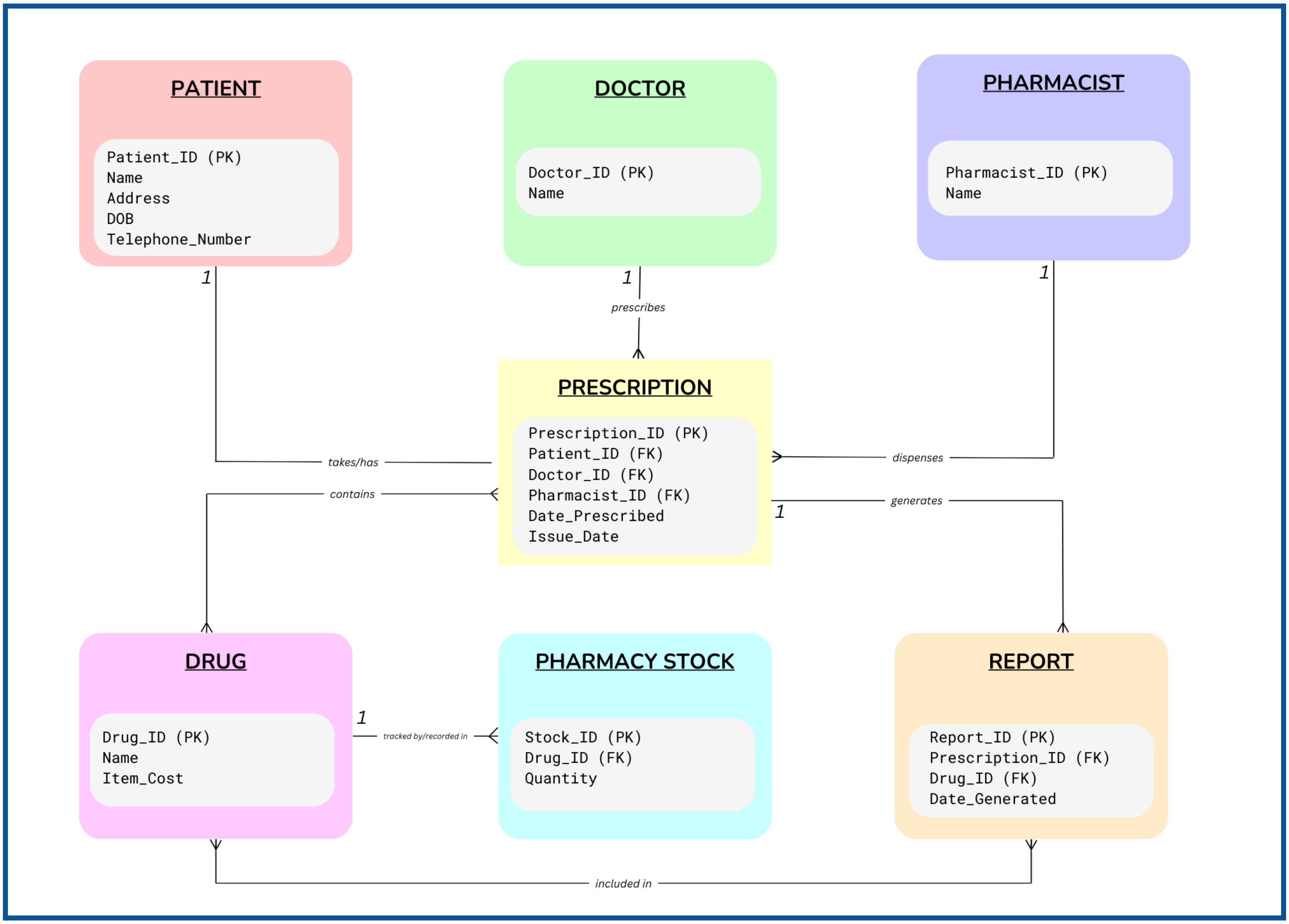
Phishing is another significant threat to Smith and Co, especially for credential harvesting. Small businesses are often more vulnerable due to limited employee training on cybersecurity, making phishing tactics, like fraudulent emails, effective. Successful phishing attacks can give attackers direct database access, enabling them to extract sensitive data like customer emails, transaction histories, and possibly employee records. To mitigate this risk, Smith and Co should conduct regular training to raise awareness of phishing techniques and enforce multi-factor authentication (MFA) for database access. MFA adds a critical layer of security by requiring additional verification, reducing the chance of unauthorised access even if credentials are compromised (CISA, 2023; NIST, 2023).

The Smith and Co bookshop database holds valuable information that makes it vulnerable to attackers, particularly because of limited security measures typical in small businesses. SQL Injection and Phishing are two prominent threats that could compromise this data. To mitigate these risks, Smith and Co should employ strong input validation, parameterised queries, regular cybersecurity training, and multi-factor authentication. By adopting these measures, Smith and Co can protect their data, maintain customer trust, and secure their operations effectively.

Task 2: St. John’s Hospital

Entity-Relationship Diagram

The following Entity-Relationship Diagram (ERD) represents the proposed database system for St. John's Hospital pharmacy. It aims to modernise and digitise the hospital's current paper-based filing system to improve data accessibility, integrity, and efficiency for pharmacy staff. The ERD outlines key entities such as Patient, Doctor, Pharmacist, Prescription, Drug, Pharmacy Stock, and Report, detailing their relationships and cardinalities.

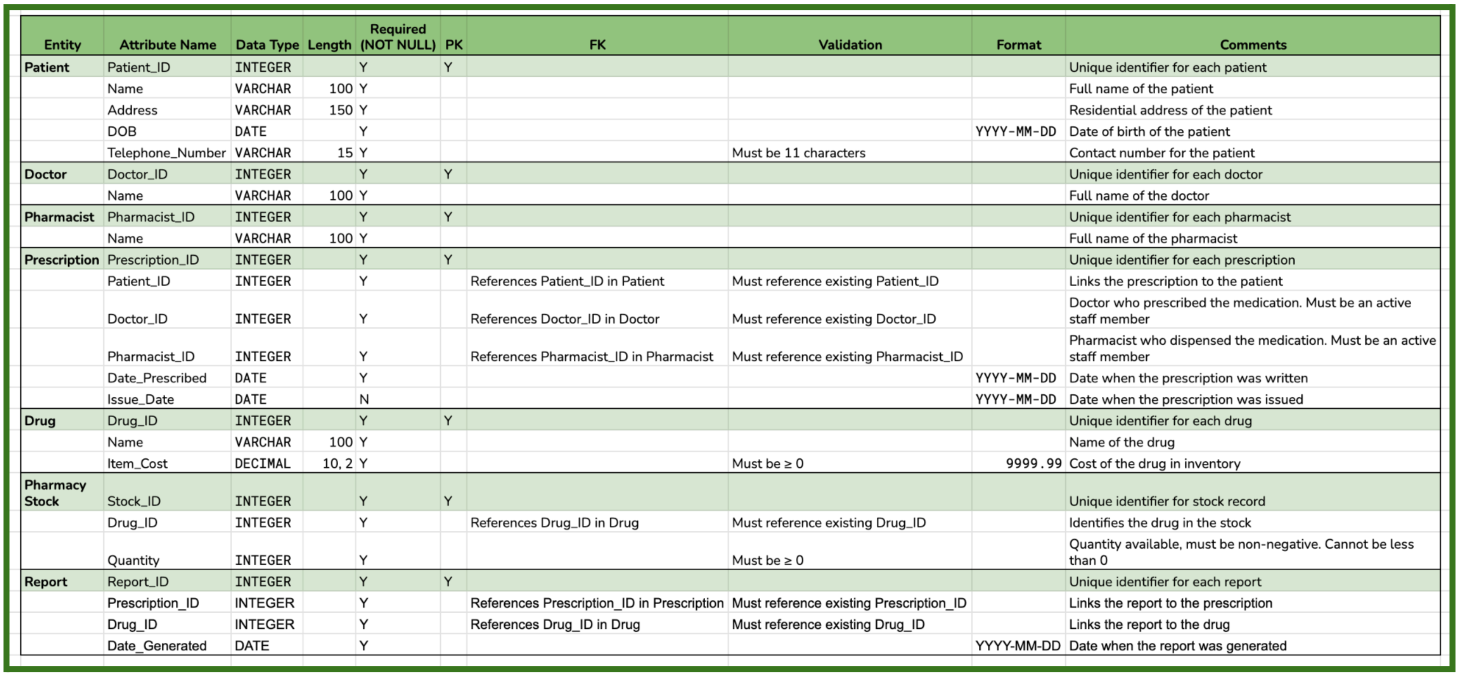


Assumptions Made in Creating the ERD

- **Unique Identifiers:** Each major entity (e.g., Patient, Doctor, Pharmacist, Prescription, etc.) contains a unique identifier to ensure there are no ambiguities in relationships.
- **Reporting Entity:** A Report entity has been added to support tracking and analysis of prescriptions and stock levels, facilitating operational insights.
- **Cardinality Assumptions:**
    - A Patient can have multiple Prescriptions, but each Prescription is linked to a single Patient.
    - Each Prescription can be prescribed by a Doctor and dispensed by a Pharmacist, allowing multiple Doctors and Pharmacists to be involved in treating various patients.
    - Pharmacy Stock is directly linked to Drug, maintaining real-time visibility of inventory.
    - The Report entity is linked to both Prescription and Drug to facilitate comprehensive tracking of issued drugs and associated prescriptions.
- **Data Relationships:** Relationships have been defined to ensure the accuracy of interactions, such as each Drug being linked to multiple records in the Pharmacy Stock table.

Data Dictionary

The following data dictionary is designed to support the new digital database system for St. John's Hospital pharmacy. It includes all the key entities, attributes, and relationships necessary for managing patient information, prescriptions, drug stock, and reporting. The dictionary details each entity in the system—from Patient records to Drug inventory and Prescription data—ensuring efficient tracking and management of information critical to hospital pharmacy operations. The Report entity has also been added to facilitate detailed tracking and analysis of prescriptions and dispensed drugs. This structured representation will ensure that the hospital’s data is managed in an accurate, secure, and efficient manner, fully supporting modernisation efforts.



Entity	Attribute Name	Data Type	Length	Required (NOT NULL)	PK	FK	Validation	Format	Comments
Patient	Patient_ID	INTEGER		Y	Y				Unique identifier for each patient
	Name	VARCHAR	100	Y					Full name of the patient
	Address	VARCHAR	150	Y					Residential address of the patient
	DOB	DATE		Y				YYYY-MM-DD	Date of birth of the patient
	Telephone_Number	VARCHAR	15	Y			Must be 11 characters		Contact number for the patient
Doctor	Doctor_ID	INTEGER		Y	Y				Unique identifier for each doctor
	Name	VARCHAR	100	Y					Full name of the doctor
Pharmacist	Pharmacist_ID	INTEGER		Y	Y				Unique identifier for each pharmacist
	Name	VARCHAR	100	Y					Full name of the pharmacist
Prescription	Prescription_ID	INTEGER		Y	Y				Unique identifier for each prescription
	Patient_ID	INTEGER		Y		References Patient_ID in Patient	Must reference existing Patient_ID		Links the prescription to the patient
	Doctor_ID	INTEGER		Y		References Doctor_ID in Doctor	Must reference existing Doctor_ID		Doctor who prescribed the medication. Must be an active staff member
	Pharmacist_ID	INTEGER		Y		References Pharmacist_ID in Pharmacist	Must reference existing Pharmacist_ID		Pharmacist who dispensed the medication. Must be an active staff member
	Date_Prescribed	DATE		Y				YYYY-MM-DD	Date when the prescription was written
	Issue_Date	DATE		N				YYYY-MM-DD	Date when the prescription was issued
Drug	Drug_ID	INTEGER		Y	Y				Unique identifier for each drug
	Name	VARCHAR	100	Y					Name of the drug
	Item_Cost	DECIMAL	10, 2	Y			Must be ≥ 0	9999.99	Cost of the drug in inventory
Pharmacy Stock	Stock_ID	INTEGER		Y	Y				Unique identifier for stock record
	Drug_ID	INTEGER		Y		References Drug_ID in Drug	Must reference existing Drug_ID		Identifies the drug in the stock
	Quantity	INTEGER		Y			Must be ≥ 0		Quantity available, must be non-negative. Cannot be less than 0
Report	Report_ID	INTEGER		Y	Y				Unique identifier for each report
	Prescription_ID	INTEGER		Y		References Prescription_ID in Prescription	Must reference existing Prescription_ID		Links the report to the prescription
	Drug_ID	INTEGER		Y		References Drug_ID in Drug	Must reference existing Drug_ID		Links the report to the drug
	Date_Generated	DATE		Y				YYYY-MM-DD	Date when the report was generated

Length: Specifies the maximum size allowed for VARCHAR and DECIMAL data types.

Required (NOT NULL): Indicates 'Y' if the column must contain a value, thereby ensuring that essential information is not left blank.

Validation: Details any business constraints or logical checks, such as ensuring references to existing IDs or positive values for quantities.

Format: Specifies constraints on data format, such as dates using the YYYY-MM-DD format.

PK (Primary Key): Identifies attributes that uniquely identify each record within a table.

FK (Foreign Key): Specifies whether an attribute is a foreign key and indicates the related table/attribute to maintain referential integrity between entities.

Comments: Provides additional information about each attribute, including its role and relevance, to assist developers and stakeholders in understanding how the data model is constructed.

References

1. CISA. (2023). Phishing: Recognize and Avoid. Available at: https://www.cisa.gov/publication/phishing (Accessed: 22 November 2024).
2. OWASP. (2023). SQL Injection Prevention Cheat Sheet. Available at: https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html (Accessed: 19 November 2024).
3. NIST. (2023). Guidelines on Security and Privacy in Public Cloud Computing. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf (Accessed: 22 November 2024).

Originals

Task 1: Smith and Co Second-Hand Bookshop - Normalisation Table

Task 2: St. John’s Hospital - Entity-Relationship Diagram

Task 2: St. John’s Hospital - Data Dictionary