Homework 2: Secure Cloud Infrastructure Design

Topic: Infrastructure Security & Architecture

Scenario: "HealthHive" (The Medical App Startup)

The Scenario

HealthHive is migrating its application from a single physical server in the CEO's garage to the **AWS Cloud**. The app consists of a **Web Server** (frontend), an **App Server** (backend logic), and a **Database** (patient records).

The Problem: The CEO wants to put everything in one big "public" bucket to make it easy to manage.

Your Job: As the Lead Security Architect, you must stop this. You need to design a **3-Tier Secure Network Architecture** that protects the patient data while keeping the website accessible to the internet.

Part 1: The Network Topology Diagram

Task: Draw a high-level network diagram of the new HealthHive infrastructure. You can use tools like Draw.io, Lucidchart, or even a clear hand-drawn sketch.

Your diagram must include and clearly label:

1. **The Internet Gateway:** Where traffic enters.
2. **Public Subnet (DMZ):** Which components belong here? (Hint: The things that need to talk to the internet).
3. **Private Subnet:** Which components belong here? (Hint: The things that hold the secrets).
4. **Security Controls:**
    - Where would you place a **Web Application Firewall (WAF)**?
    - Where would you place the **Load Balancer**?
    - Where would you place the **Database (RDS)**?

Hint for Students: Think about "Defense in Depth." If a hacker compromises the Web Server in the Public Subnet, what stops them from immediately stealing the Database in the Private Subnet?

Part 2: The Security Control Stack

Task: For each layer of your infrastructure, identify **ONE** specific security control you would implement and explain **WHY** in 1-2 sentences.

Infrastructure Layer	Security Control (Tool/Concept)	Why is this necessary?
Edge (Entry)		
Network		
Server (Host)		
Cloud Config		
Data (Storage)		

Choose from concepts discussed in class: *WAF, NACL/Security Groups, EDR, CSPM, Encryption at Rest, IAM Roles, Jump Box/Bastion Host.*

Part 3: Disaster Recovery Strategy

Scenario: A ransomware gang manages to encrypt your main Database. They are demanding 50 Bitcoin to decrypt it.

Task: Outline your **Backup & Recovery Strategy** using the **3-2-1 Rule** learned in class.

1. **The 3-2-1 Configuration:**
    - **3 Copies:** (e.g., Live Data, Local Backup, Cloud Backup).
    - **2 Media Types:** (e.g., SSD, S3 Bucket).
    - **1 Offsite/Immutable:** Describe how you will ensure the ransomware cannot delete your backups. (Hint: Look up "S3 Object Lock" or "Immutable Backups").
2. **Recovery Time Objective (RTO):** The CEO asks, "How fast can we get back online?"

- Define a realistic RTO for this startup (e.g., 4 hours, 24 hours) and explain the trade-off between speed and cost.

Bonus: Explain why HealthHive should use **Infrastructure as Code (IaC)** (like Terraform) instead of manually clicking buttons in the AWS Console to build this.