Acme HealthTech is a mid-sized healthcare company with 150 employees. It operates a web-based patient portal, internal HR system, and cloud-based email. As a healthcare company, it must comply with HIPAA and ensure data privacy and availability.”

| **Asset** | **Description** | **Owner** | **Confidentiality** | **Integrity** | **Availability** |
| --- | --- | --- | --- | --- | --- |
| Patient Portal | Web app for accessing patient data | IT Department | High | High | High |
| HR System | Employee data & payroll system | HR Manager | Medium | Medium | Medium |
| Email Platform | Staff communication tool | IT Department | Medium | Medium | High |

| **Asset** | **Threat** | **Vulnerability** | **Likelihood** | **Impact** | **Risk Level** |
| --- | --- | --- | --- | --- | --- |
| Patient Portal | Data breach | Weak access controls | High | High | High |
| HR System | Insider misuse | No access logs | Medium | Medium | Medium |
| Email Platform | Phishing attack | No email filtering | High | Medium | High |

**Recommend Controls**

1. **Patient Portal:**  
   To reduce the risk of data breaches, implement **multifactor authentication (MFA)** and **role-based access control (RBAC)** to ensure only authorized users access sensitive data. Conduct **regular vulnerability assessments and penetration testing** to uncover weaknesses in the web application. Additionally, ensure data is encrypted both at rest and in transit.
2. **HR System:**  
   To prevent insider misuse, enable **detailed audit logging and monitoring** of user activity. Ensure **least privilege access** is enforced so employees can only access data necessary for their roles. Conduct **background checks and security awareness training** for HR staff handling sensitive data.
3. **Email Platform:**  
   Deploy **advanced email filtering solutions** to block phishing and malicious attachments. Implement **user awareness training** to help staff identify and report suspicious emails. Enforce **DMARC, DKIM, and SPF** email authentication standards to prevent spoofing.
4. **All Systems:**  
   Establish a **centralized incident response plan** to ensure a timely response and containment of threats across all assets. Perform **routine patch management** to fix known vulnerabilities in systems and applications.
5. **Network-Level Protection:**  
   Use **network segmentation** to isolate critical systems like the Patient Portal and HR System from general internet traffic. Deploy **intrusion detection and prevention systems (IDPS)** to monitor and block malicious activities at the network level.