INTERNATIONAL CYBERSECURITY AND DIGITAL FORENSICS ACADEMY

GRC104-P2 Paper 2: Practical Competency Skills Test

Student Name:

Oluwagbemi Oluwatimilehin

Registration Number:

2025/GRC/10712

Date: 21-11-2025

Table of Content

Executive Summary

Dr. Larouche's dental practice is growing also with consideration of moving the IT services to the cloud, but it is facing major challenges in Governance, Risk, and Compliance. Currently, there are some weaknesses associated with the current practice such as shared administrative access, unencrypted backup drive, outdated protocols, missing security updates which exposes the electronic protected health information (ePHI) to potential security / data breaches.

The consideration of adopting cloud services of ClouDDS poses a third-party risk which require intense due diligence, risk assessment and HIPAA compliant.

This report addresses the major challenges faced by Dr. Larouche's dental practice with control measures.

Part A: Governance, Policy, and Control Design

Task 1: HIPAA Technical Safeguards and Control Gaps

Firstly, what are technical safeguards? Technical Safeguards as defined by security rile in 164.304 is the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

Section	Standard Name	Implementation Specifications (List all applicable)	Control Gap in Dr. Larouche's Practice
164.312(a)(1)	Access Control	• Unique User Identification (Required) • Emergency Access Procedure (Required) • Automatic Logoff (Addressable) • Encryption and Decryption (Addressable)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.
164.312(c)(1)	Integrity	Mechanism to authenticate electronic protected health information	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
164.312(e)(1)	Transmission Security	• Integrity Controls (Addressable) • Encryption (Addressable)	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

Task 2: Policy Excerpt Drafting – Password Policy

Password and Authentication Policy Excerpt for Dr. Larouche's Dental Practice

Purpose:

Passwords are essential aspect of computer security; they also serve as the front line of protection for users account which contains the ePHI. A compromised password may lead to security breach in the organization's network. All staff are to be responsible for taking appropriate steps to select and secure their passwords. The purpose of this policy is to reinforce the use of effective passwords, also categorised as "Strong Passwords," and require all staff members to change their passwords regularly.

Policy Description:

The information systems used in accessing the ePHI of clients will be programmed to uniquely identify and authenticate staff members through the use of strong passwords. to confirm that only authorized member accesses the information system used to access the ePHI of clients:

- The organization shall assign unique user ID and passwords to staff members
- The organization shall integrate a biometric identification system enhancing a multifactor authentication mechanism for administrative access to the system.

Unique User ID and Password Management:

- Upon receipt of unique user ID and password, each staff are expected to change the password provided to the password only he/she knows to ensure confidentiality of their passwords
- Exposed password to any other staff member must be changed immediately
- No exchange of passwords among staff members.
- Passwords must be changed every six months

Password Guidelines (Using NIST SP 800-63B Guideline):

- Passwords length shall be a minimum of 12 characters including special characters/symbols such as @,_,&,!
- No use of common words for passwords, words like; john123, password123 etc.

Part B: Advanced Risk and Vulnerability Assessment

Task 3: Vulnerability Analysis and Risk Prioritization

ID	Vulnerability Description	Affected Asset	CVSS v3.1 score	Likelihood (1-5)	Impact (1-5)	Residual Risk Score	HIPAA Mapping
VA-001	**SMBv1 Protocol Enabled:** The server is running the deprecated and	EHR Server	9.8	5	5	24	164.312(a)(1)

	insecure Server Message Block (SMB) version 1 protocol.						
VA-002	**Weak Password Policy:** Local accounts (including AdminUser) are configured to allow passwords shorter than 8 characters and do not enforce complexity.	EHR Server	7.5	4	4	15	164.312(a)(1)
VA-003	**Unencrypted Backup Drive:** The external USB drive used for nightly backups is not encrypted.	EHR Server	8.6	5	5	24	164.312(e)(2)(ii) 164.312(a)(2)(iv)
VA-004	**Missing Security Updates:** The operating system is missing patches released 90 days ago, including a	Staff Workstation	9.0	4	5	19	164.312(c)(1)

	critical patch for a remote code execution (RCE) flaw.						
VA-005	**Unrestricted Guest Wi-Fi Access:** The Guest Wi-Fi network is on the same subnet as the staff network and EHR server. EHR Server	Network	6.5	3	4	11	164.312(a)(1)

Task 4: Risk Treatment Plan

ID	Vulneraility Descriotion	Residual Risk Score	Treatment Strategy	Specific Mitigation Action
VA-001	**SMBv1 Protocol Enabled:** The server is running the deprecated and insecure Server Message Block (SMB) version 1 protocol.	24	Mitigate (this risk can only be mitigated because SMB is a communication protocol that enables communication between remote system, the vulnerability cannot be	Disable SMBv1 Protocol using the server manager GUI or via PowerShell. Upgrade to the latest version of SMB Protocol. Conduct regular monitoring, and upgrade regularly.

			accepted as it poses major risk to the server)	
VA-003	**Unencrypted Backup Drive:** The external USB drive used for nightly backups is not encrypted.	24	Mitigate (the backup drive is essential, it contains sensitive information of clients, the risk can only be mitigated using strong encryption)	Implement Strong Encryption. Store Backup Drive in a secure location. Restrict access to the backup drive, only authorized personnel should have access to it.

Post-Mitigation Residual Risk:

Recalculating the Residual Risk Score:

VA-001; Likelihood = 5, Impact =5, Control Effectiveness = 4

RRS = (Likelihood x Impact) – Control Effectiveness

Therefore, VA-001 RRS = (5 x 5) – 4 = 21

VA-003; Likelihood = 5, Impact =5, Control Effectiveness = 4

RRS = (Likelihood x Impact) – Control Effectiveness

Therefore, VA-003 RRS = (5 x 5) – 4 = 21

Part C: Third-Party Risk Management (TPRM)

Task 5: Vendor Due Diligence

Required Documentation for Due Diligence:

- Business Associate Agreement
- Risk Assessment Report or Audit
- Policies and Procedure (Security and Privacy)

Critical Control Review:

- Access Control: this control is critical as it serves as a baseline in protecting ePHI of clients. According to HIPAA Technical Safeguard, Access control 162.312(a)(1) is the abiity or means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. A covered entity or business associate must comply with this control as it enables that only authorized users have access to minimum necessary nformation needed to perform their job function, because if an unauthorized person have access to sensitive information it might lead to HIPAA breaches.

- Audit Control: this control is critical as it tracks access to ePHI, detect unauthorized access, or prove compliance which shows how they respond to incidents in case of security breach.
- Integrity control: this control is critical as it ensures that data/information of clients have not be altered or modified.

Task 6: Business Associate Agreement (BAA) Analysis

Key BAA Clauses:

- Safeguard Clause detailing the security measures the business associate must implement to protect ePHI, the measures must include; Administrative safeguards, Technical Safeguards and Physical Safeguards.
- Reporting Obligation Clause this specifies how and when the business associate must notify the covered entity about any security incident or breach.
- Permitted Use and Disclosure Clause this clause determine how the business associate can use or share ePHI.

BAA Breach Notification:

- CloudDDS must notify Dr. Larouche in maximum of **60 days** after the discovery of a data breach.
- Dr. Larouche must notify affected patients and HHS in maximum of **60 days** after the discovery of a data breach.

Part D: Incident Response and Business Continuity

Task 7: Incident Response Plan (IRP) Development

Five key phases of the Incident Response Lifecycle:

- Preparation
- Detection and Analysis
- Containment
- Eradication and Recovery
- Post-event activity

In the case of the theft of the external USB backup drive (VA-003), the first critical step the staff must take is to report and escalate the incident to the Privacy or Security officer as the case may be and also record the incident in the incident management system. this step will enable the Privacy / Security Officer carry out assessment on the stolen external USB backup drive, the assessment that shall be conducted will include;

- To determine which ePHI was exposed or will be exposed
- How many patients will be affected if the data is exposed
- The type and sensitivity of the data contained in the external USB backup drive
- What can be done to quickly mitigate the breach

The other critical action to be taken in the first four hours is that, staff must ensure that they initiate early containment of the event because the drive stolen is unencrypted, thereby the potential risk is high, early containment is needed to mitigate the risk, then there must be evidence preservation which must be included in HIPAA documentation, internal audit, the area whereby the theft occurred must be secured, no one goes in or out until the evidence is preserved and proper investigation is done.

Task 8: Business Continuity and Recovery

Recovery Strategy:

- Isolation of infected systems to contain the breach.
- Restoration of ePHI from USB backup drive.
- Hardening and password reset
- Restore full operation

Lessons Learnt:

- Strong password and authentication policy
- Patching and vulnerability management
- Encryption of Backup Drives