INTERNATIONAL CYBERSECURITY AND DIGITAL FORENSICS ACADEMY

ACI-805 : The Investigator's Crucible

REG. NUMBER: 2025/ACI/9958

NAME : Ambreena Munir

Date: 14 September, 2025

Instructor: Aminu Idris

Part 1 : The Ethical Compass

1) Multi-Framework Analysis

- **Deontolog (duty / rules):** What is your absolute duty in this situation? What universal rule applies?
  - The absolute duty is that I have to follow law and bound of legal authorization.
  - According to rules do not access and search data without lawfull authorization.
  - In case of accepting the Brenda's password would violate a rules, risk illegal search and professional licensing consequences. So my obligation should be to refuse unauthorized access and report the offer through appropriate legal channels.

- **Utilitarianism (consequences / greatest good):** What are the potential costs and benefits of accepting the password? Which action produces the "greatest good for the greatest number"?
  - Potential benefits of accepting the password is the faster discovery of stolen code, stop harm to Innovate Corp and save company.
  - Potential cost should be illegaly obtained evidence could be excluded in court, damage to employee trust and effect on privacy.
  - While short-term benefits exist, the downstream legal, reputational and systemic harms may outweigh the immediate benefits. So the utilitarian argument is probably in favor of not using passwords unless legal authorization is obtained.

- **Virtue Ethics (character / professional virtues):** What would a professional of integrity, discretion, and honesty do? Which virtues are at stake?
  - Refuse to conduct an unauthorized search, work transparently with the legal/compliance team, protect both the integrity of the investigation and Brenda's safety (avoid exposing her to retaliation), and seek lawful means (warrant, consent) to pursue charges. Use of passwords would show a lack of professional discretion and risk corrupting justice.

2) Personal Conviction & Dissenting Opinion

- **Your Decision:** State clearly whether you would accept the password or not. Justify your choice by declaring which ethical framework you find most compelling in this specific case. Explain why your personal and professional judgment aligns with this framework over the others.
  - I would not accept Brenda's password. My primary duty is to obey the court order and legal constraints that authorize the investigation. Unlawful searches are wrong regardless of intended outcomes.
  - Utilitarianism may allow rules to be broken if it seems it will bring the greater good, but this is risky because future consequences are uncertain. Potential legal problems such as losing a case, liability, or reputational damage make such shortcuts dangerous.
  - Virtue ethics focuses on being a good and honest person but does not clearly state what actions to take immediately. Deontology, on the other hand, gives clear rules that match professional duties and help prevent the chain of harms that both utilitarianism and virtue ethics are concerned about.

- **The Dissenting Opinion:** Write a short, powerful paragraph from the perspective of the ethical framework you rejected. Argue passionately why your chosen course of action is wrong, misguided, or dangerous. This demonstrates your ability to understand and respect opposing viewpoints, even when you disagree.
  - Refusing to use Brenda's password when vital company codes are at risk could be considered ethically wrong. Immediate harm such as ongoing theft, a competitor gaining leverage, potential layoffs, or loss of customer confidence – can seriously harm the company and many innocent people. If using passwords can prevent theft, recover stolen data, and protect employees and customers, it may be worth breaking the rule. The goal of ethics should be to minimize harm and maximize overall good. In urgent situations where legal steps take too long, strictly following the procedure may cause more harm. Acting with compassion means taking the opportunity to prevent as much harm as possible.

Part 2: The Legal Gauntlet

Preliminary Investigative Action & Risk Report

Incident: *"PharmaLeek" Data Breach*
Prepared For: General Counsel, Global Health Pharma (GHP)
Prepared By: Lead Investigator, Cybersecurity Forensics Division
Date: 14th Nov, 2025

1. Executive Summary

Global Health Pharma (GHP) has suffered a major cross-border data breach originating from a vulnerable web server in its Frankfurt, Germany office. The attacker exploited an unpatched vulnerability – a patch was available for three months – to gain unauthorized access to sensitive research data related to a new Alzheimer's drug, as well as the personal health information of 5,000 clinical trial participants.

The exfiltrated data has been discovered on a staging server in Toronto, Canada, suggesting ongoing or complete transfer to external threat actors. The dataset includes personal data of EU citizens (≈40%) and health records of California residents (≈10%), applying multiple data protection laws.

A secondary, unrelated discovery indicated that a GHP employee had used the same Frankfurt server for an illegal online sports betting operation, which should have been handled separately and ethically under incidental search protocols.

Following immediate risk are:

- Potential violation of GDPR, HIPAA, and CCPA due to exposure of sensitive health and personal data.
- Regulatory fines, lawsuits and reputational damage in multiple jurisdictions.
- There is obvious contamination risk if incidental findings are not properly controlled.

Recommended direction:

- To properly store and preserve evidence.
- Involve the relevant data protection authorities in the EU, US and Canada.
- Initiate cross-border legal cooperation (possibly through MLAT).

2. Jurisdictional & Legal Compliance Analysis

Framework / Law	Why It Applies	Immediate Obligations / Deadlines
General Data Protection Regulation (GDPR) – EU (primarily Germany & France)	40% of affected patients are EU citizens. GHP processes personal and health data of EU residents, making it a *data controller.*	• Notify the German Data Protection Authority and affected individuals within 72 hours of becoming aware of the breach. Conduct a Data Protection Impact Assessment (DPIA). Ensure lawful cross-border data transfer procedures.
Health Insurance Portability and Accountability Act (HIPAA) – United States	The exfiltrated data includes health-related clinical trial information collected by a US-based entity, classifying it as Protected Health Information (PHI).	Breach notification to affected individuals and the HHS Office for Civil Rights within 60 days of discovery. Maintain documentation for six years. Implement immediate administrative, physical, and technical safeguards.
California Consumer Privacy Act (CCPA) / CPRA	10% of affected patients are California residents. Their personal data, including health data, falls under CCPA jurisdiction.	Notify the California Attorney General and affected residents "in the most expedient time possible." Allow consumers to request data deletion or information on data disclosure.
Canadian Privacy Law (PIPEDA)	The staging server is located in Toronto, where data is being processed or stored.	Report the breach to the Office of the Privacy Commissioner of Canada as soon as possible. Maintain a breach record for 24 months. Notify affected individuals directly if there is "a real risk of significant harm."
Mutual Legal Assistance Treaty (MLAT) Considerations	Data resides in multiple jurisdictions (Germany → Canada → US).	Initiate MLAT procedures via national law enforcement channels (e.g., FBI, RCMP,

		BKA) to lawfully collect evidence and share data across borders. Avoid direct extraction from the Canadian server without proper authority.

3. Investigative Strategy & Ethical Safeguards

Next Three Critical Steps

1. Evidence Containment and Preservation

- Action: Forensically image the compromised Frankfurt server, collect logs and preserve volatile data (RAM, network connections).
- Due Care: Maintain records of the entire chain of custody. Use write blockers, generate SHA-256 hash values, and store images in tamper-evident containers.
- Goal: To ensure the integrity and admissibility of digital evidence under EU and US evidence standards.

2. Cross-Border Coordination and Legal Notification

- Action: Coordinate with legal counsel and data protection authorities to submit mandatory breach notifications under GDPR, HIPAA, and CCPA.
- Due diligence: Limit data transfer to authorized entities. Engage government agencies through MLAT to retrieve data from Canadian servers.
- The goal: Maintain compliance while ensuring that there is no unauthorized international data movement.

3. Threat Actor Attribution and Containment

- Action: Analyze the extracted dataset, establish Indicators of Compromise (IOC), and identify the attacking infrastructure.
- Due care: Modify or anonymize patient identifiers during threat analysis to protect privacy. Follow least privilege and data minimization principles.

- The goal: prevent further data loss, identify responsible parties, and support potential prosecution.

Ethical Procedure:

- Document the findings without accessing or expanding the scope of unrelated activity.
- Immediately notify the General Council of GHP and suspend analysis of this data stream.
- Look for written authorization or a new court order if further review is needed.
- Store logs and evidence separately to maintain legal admissibility and avoid "scope creep."

Why this matters:

Deviating from this process could invalidate the entire breach investigation, violate customer trust, and corrupt evidence – making both the betting evidence and the breach data inadmissible in court. It could also expose GHPs and investigators to claims of unauthorized surveillance or privacy violations.

4. Internal Failures Assessment

Based on initial analysis, GHP's breach stems primarily from lack of due diligence and deficient vulnerability management:

Failure Area	Assessment
Patch Management	The exploited web server vulnerability had a patch available for 3 months a clear failure of timely patching and risk prioritization.
Security Governance	Absence of a centralized monitoring or compliance audit system to verify patch compliance across regions.
Incident Preparedness	GHP appears to lack a tested incident response plan, leading to delayed detection and reporting.

Access Control Oversight	The same server being misused for illegal betting indicates poor access monitoring and violation of acceptable use policies.

Conclusion:

The breach occurred due to poor maintenance, oversight, and response planning as was the case with the Equifax breach. GHP should fix its patching process, regularly monitor all servers, and train staff on proper system use.

Part 3: Formal Response to the (ISC)² Ethics Committee

To: (ISC)² Ethics Committee
From: Ambreena Munir, Lead Investigator
Date: 14th Nov, 2025
Subject: Response to Complaint Regarding the "PharmaLeek" Investigation

Addressing Allegation 1: Handling of the Illegal Betting Ring

The first charge claims that I acted negligently by recommending GHP contact law enforcement about an illegal betting operation, potentially informing the primary attacker and violating employee confidentiality.

My Response:

- The betting operations were discovered incidentally during a legitimate investigation of the data breach. I did not access or expand beyond the scope of the initial investigation without authorization.
- In accordance with proper ethical procedure, I immediately reported the findings to the General Council of GHP, and stored all evidence separately. I did not take any independent enforcement action.
- This decision is in line with Canon 1 of the (ISC)² Code: "Protect society, the common good, essential public trust and confidence." By reporting illegal activity, I protected society and the organization from further criminal behavior.

- It also aligns with Canon 3: "Provide diligent and competent service to the principals." My primary duty to GHP required me to alert the company while balancing confidentiality and legal boundaries. By separating the incident from the main breach, I maintained confidentiality and integrity while fulfilling my responsibility to protect the organization.

Conclusion: My actions were careful, ethical and consistent with professional duties. I prioritized legal compliance, ethical reporting, and risk mitigation while protecting confidentiality as much as possible.

Addressing Allegation 2: Server Outage

The second allegation concerns a **15-minute server outage** caused during forensic imaging.

My Response:

- The short server outage was an unexpected technical problem. We followed proper procedures, used approved equipment and planned for potential risks.
- Following Canon 3, we acted competently by ensuring that the investigation was accurate and the evidence remained intact. The outage was very small, repaired quickly and no data was lost.
- Following Canon 4 (“Advance and Protect the Profession”), we recorded what happened, reviewed our process, and added safeguards to prevent it from happening again. This helps maintain professional standards and share lessons with the team.

Conclusion: The outage was not due to a lack of skills or ethics. This was a rare, unavoidable technical problem which was dealt with carefully and professionally.

Concluding Statement of Professionalism

I reaffirm my commitment to the ethical principles of cybersecurity: honesty, integrity, respect for privacy and the protection of the public. My decisions during the “Pharmaleek” investigation were guided by law, professional codes and best practices to protect data, society and organizational trust. I am accountable for my actions and dedicated to maintaining the highest standards of the profession.

Part 4: Letter to My Younger Self

Dear Younger Me,

Congratulations on your first day as a cyber crime investigator! You are full of technical knowledge and enthusiasm, but one lesson I want to share is more important than any tool, script or exploit: your integrity is your compass.

Think of it like walking a tightrope across a deep valley. Every technical skill you have has a safety net underneath, but the only thing keeping you steady on the rope is your internal compass – your moral judgment. One wrong move, one shortcut, and you could fall – not just professionally, but morally as well. You will encounter situations where breaking a rule seems to be the fastest way to solve a problem. This may be accessing data without permission, or causing the customer to perform actions before they are ready. The rope will wobble, but if you trust your compass, you will always land safely.

Throughout your career, you will discover that legality and ethics are not always the same thing. Laws may lag behind technology, and policies may not cover every scenario. Your job is to do what's right, not just what's allowed. Keep data safe, keep people safe, and protect yourself by documenting everything, moving forward when unsure, and never wavering even under pressure.

Remember, reputation is fragile. One ethical mistake can undo years of great work. But when you work with integrity, you gain trust, respect, and the ability to make a meaningful impact. The world of cybersecurity rewards skill, but it prizes character even more.

So step onto the rope with confidence, hold tight to your compass and always let your judgment guide you. The career you build will not be defined by how fast you work, but by how well you do it.

Sincerely,

Ambreena Munir