**Department of Computer Science**

**( Cyber Security )**

**MENAL NOOR**

**Information Assurance**

**Topic: Cybersecurity Breach Analysis and Pakistan Privacy Laws Review**

**Q1: Healthcare Payment Platform Breach**

* 1. **List of violations**

**Credit Card Rules (PCI DSS):**

* **Encryption:** One of the rules under PCI DSS is to protect credit card information by using encryption. This indicates that the data cannot be read by anyone who gains access to it because it is muddled. However, the company did not use encryption to safeguard the stored card data in this instance. This is against the PCI DSS guidelines.
* **Data protection**: Securely storing credit card data is another PCI DSS rule. The company should have made sure that the card data was not stored in a way that could be easily stolen. Since the company didn’t do this, it is violating PCI DSS again.

**HIPAA (Health Information Rules):**

* **No Protection for Health Information**

HIPAA stipulates safeguards for medical records of patients. The confidentiality and safety of patient health information is one of the rules. However, the company did not adequately safeguard patient records in this instance. HIPAA is being broken in this way. GDPR (European Union Rules):

* **Unnecessary Data Collection:**

GDPR has a rule called “data minimization,” which means that companies should only collect the personal data they need to do their job. However, the company in this instance gathered more health information than was necessary. This is a violation of the GDPR rules.

* 1. **Penalties ( Fines )**
* **PCI DSS:**

A violation of PCI DSS regulations could result in a monthly fine of $5,000 to $100,000 until the issue is resolved. The amount depends on how serious the violation is.

* **HIPAA:**

Under HIPAA, if a company breaks the rules, they could be fined $100 to $50,000 for each mistake, with a maximum fine of $1.5 million in a year. The company could also face other penalties if they don’t fix the problem.

* **GDPR:**

One of the most stringent data protection laws is GDPR. If a company breaks the rules, they could be fined up to €20 million or 4% of their global yearly income (whichever is higher). This is a very large fine.

* **Which Law Will Likely Impose the Highest Penalty?**

The law that is most likely to impose the highest fine is GDPR. This is because GDPR has one of the highest penalties for violations. If a company breaks GDPR rules, they could face a fine that could be up to 4% of their total worldwide income. That can be a significant sum, particularly for large businesses.

* 1. **Fix the issues**

**Regarding the PCI DSS (Credit Card Rules):**

**1.Use Encryption:**

The company should use encryption to protect credit card data. The data is encrypted in such a way that even if a hacker obtains it, they will be unable to read it.

**2.Use Stronger Passwords:**

The company should make sure that employees use stronger passwords to protect data. To prevent hackers from gaining access, employees should change their passwords frequently and not use passwords that are simple to guess.

**Health Information Security Act (HIPAA):**

**1.Create a Security Policy:**

The company should create a policy to protect patient health information. All health data should be encrypted (scrambled) and employees should use strong passwords to keep it safe, according to this policy.

**For GDPR (EU Data Rules):**

**•Rule for Data Storage:**

The company should create a rule saying that health data must be encrypted and stored only for as long as needed. After that, it should be safely deleted. The company should only keep the information they need to provide their services and protect the data.

* 1. **Critical thinking:**

**Can strict regulations stop all violations?**

• No, even if a company adheres to stringent regulations, it may still encounter security issues. Rules help lower the chances of a breach, but they can’t completely stop hackers or prevent human mistakes. Employees may continue to click on phishing emails, or hackers may discover new methods for breaking into systems. Having strict regulations, on the other hand, makes it harder for hackers to steal sensitive data.

**What is the conflict between HIPAA and the PCI DSS? How can I fix it?**

**•Conflict**: PCI DSS has rules for storing and protecting credit card information, and HIPAA has rules for protecting patient health information. The problem is that they both have different rules for storing sensitive data. For instance, HIPAA may mandate distinct guidelines for the management of health records, while PCI DSS may mandate particular types of encryption.

**•How to Fix It:** The company should separate health and credit card data to fix this. The company will be able to adhere to the correct regulations for each kind of data in this manner. They can use one set of security measures for credit card data and a different set for health data. This helps make sure both rules are followed correctly.

**Q2: The Privacy Laws in Pakistan**

**1. Personal Data Protection Act (PDPA) 2023:**

**•How it Works:**

The Personal Data Protection Act (PDPA) 2023 is a law in Pakistan that tries to protect people’s personal data. The law says that companies must be careful about how they collect, store, and use people’s data. However, given that this law is brand-new, individuals and businesses may not yet be aware of all the rules. It’s also not clear if companies are really following it.

**•Comparison with GDPR (EU Rules):**

The PDPA is somewhat similar to GDPR, which is a strict privacy law in Europe. However, the PDPA is not as strong as GDPR because it doesn’t have as many specific rules about how companies should handle personal data. Also, it doesn't have strong enough penalties or enforcement, so it may not be as effective as GDPR.

**2. Prevention of Electronic Crimes Act (PECA) 2016:**

**•How it Works:**

PECA is a law that helps stop cybercrimes like hacking, online fraud, and identity theft. It focuses more on stopping people from doing bad things online rather than protecting people’s personal data. It doesn’t have clear rules about how to protect personal information online.

**•Comparison with GDPR**

PECA focuses on preventing cybercrime, whereas GDPR focuses specifically on protecting personal data. While PECA does not provide clear guidelines for data protection, GDPR is significantly more effective at ensuring that businesses safeguard individuals' personal information.

**3. Rights under the Constitution:**

**• How it Works:**

The right to privacy is enshrined in Pakistan's Constitution. But the Constitution doesn’t provide clear rules on how to protect people’s data in the digital world. It just says that people should have privacy, but it doesn’t explain how to keep that privacy safe in today’s online world.

**Problems:**

**Issues with Pakistan's Privacy Legislation:**

**•Not Enough Awareness:**

One big problem is that many people in Pakistan might not know about the new privacy laws. Companies and even regular citizens might not fully understand the rules or how to follow them. As a result, mistakes in handling personal data may occur.

**•Weak Enforcement:**

The laws are not being enforced strictly enough. Even though there are rules to protect people’s privacy, it’s hard to know if companies are actually following them. There aren’t enough resources to check if companies are doing things the right way.

**•Privacy in Digital Age:**

The current laws in Pakistan were made when the internet was less important. However, in today's world, we access our personal information online at all times and use the internet for almost everything. The new ways that data is being used and stored in the digital world are not always covered by these laws.

**•Comparison with GDPR:**

When compared to GDPR, which is one of the strongest privacy laws in the world, Pakistan’s laws are not as strict. GDPR has detailed rules on how to protect personal data, and companies face big fines if they break these rules. Pakistan’s laws are newer, but they don’t have the same level of detail or penalties. The fines under Pakistan's laws are smaller and less clear. Also, GDPR has clear instructions on how companies should protect personal data and what to do if there is a breach. Pakistan’s laws don’t have as much detail in these areas.