Assignment 1

Part 1: Premera Blue Cross Case

The following 3 questions refer to the Premera Blue Cross case linked below:

<https://www.hipaajournal.com/ocr-imposes-2nd-largest-ever-hipaa-penalty-of-6-85-million-on-premera-blue-cross/>

Review the case and answer the following questions.

The advanced persistent threat (APT) remained undetected for almost how long within Premera’s network?

In May 2014, an advanced persistent threat group gained access to Premera’s computer system where they remained undetected for almost 9 months.

Due to this breach, Premera Blue Cross will be closely monitored by the Department of Health and Human Services’ Office for Civil Rights for how long?

Premera Blue Cross will also be closely monitored by OCR for two years to ensure compliance with the CAP.

Did Premera have any follow up action as part of the HHS` Office for Civil Rights investigation?

Premera Blue Cross has agreed to adopt a robust corrective action plan to address all areas of noncompliance discovered during the OCR investigation.

Premera Blue Cross agreed to settle a $10 million HIPAA violation lawsuit over the breach. The health plan had been investigated by 30 state attorneys general who determined Premera Blue Cross had not met its obligations under HIPAA and Washington’s Consumer Protection Act. In 2019, Premera Blue Cross also agreed to settle a $74 million lawsuit filed on behalf of individuals whose ePHI was exposed in the breach.

Part 2: University of Texas MD Anderson Cancer Center Case

The following 5 questions refer to the University of Texas MD Anderson Cancer Center case linked below:

<https://www.hipaajournal.com/ocr-4-3-million-cmp-university-texas-md-anderson-cancer-center/>

Review the case and answer the following questions.

Does a covered entity have the right to contest HIPAA violations?

No. Individuals, organizations, and agencies that meet the definition of a covered entity under HIPAA must comply with the Rules' requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information.

The MD Anderson HIPAA violation described in the case focused primarily on what?

The risk analysis revealed the use of unencrypted devices posed a serious threat to the confidentiality, integrity, and availability of ePHI.

Did the MD Anderson facility have a policy in place regarding portable storage devices and encryption?

Yes, in 2006 MD Anderson developed policies that required all portable storage devices to be encrypted.

How long did it take the MD Anderson facility to deploy encryption in their environment after this encryption policy was created?

Encryption was not implemented until March 24, 2011, 5 Years after the policy was created.

In the referenced MD Anderson case, the laptop that was lost by Dr. Randall Millikan \_\_\_\_\_.

The laptop was stolen from the home of Dr. Randall Millikan on April 30, 2012. Dr. Millikan confirmed that the ePHI on the device were not encrypted, the laptop was not password protected, and the ePHI could potentially have been viewed by family members at his home as a result, as well as by the individual who stole the laptop.

Part 3: Summary of HIPAA Violation Cases

The following 5 questions refer to the Summary of HIPAA Violation Cases and FAQs (at the bottom of the site) linked below:

<https://www.hipaajournal.com/hipaa-violation-cases/>

Review the site and answer the following questions.

From the FAQs, HIPAA has a detailed list of training requirements that a covered entity must impose on their employees.

Other than stipulating training should be provided “as necessary and appropriate for members of the workforce to carry out their functions” (HIPAA Privacy Rule) and that CEs and BAs should “implement a security awareness and training program for all members of the workforce” (HIPAA Security Rule), there are no specific HIPAA training requirements. Therefore you should assess employees’ security awareness as part of a risk analysis to see if more training is required.

From the FAQs, an organization can be fined for the same HIPAA violation multiple times.

Yes. If an organization fails to take corrective action after having been issued a fine, the HHS` Office of Civil Rights can impose subsequent fines. An organization´s prior history with regards to HIPAA non-compliance can also be a contributory factor in the calculation of penalties for HIPAA violations and therefore a second or subsequent fine will likely be much larger than the first.

From the FAQs, how many HIPAA violation classifications and penalty tiers are there?

There are four different HIPAA violation classifications which rank the level of an organization´s “willful neglect”, and four penalty tiers depending on factors such as the length of time a violation was allowed to continue after being discovered, the number of people affected by the violation, and the nature of data exposed. An organization´s willingness to assist with an investigation is also taken into account.

From the FAQs, how many complaints and notifications of breaches does the HHS` Office for Civil Rights generally receive each year?

The HHS` Office of Civil Rights receives between 1,200 and 1,500 complaints and notifications of breaches per year. In the majority of cases, the agency resolves the complaints without the need for an investigation or finds no HIPAA violation exists. However, up to 500 cases per year result in a fine and/or corrective action being required.

The HHS` Office for Civil Rights has increased its enforcement activities in recent years resulting in a doubling of the number of financial penalties imposed in 2016. In 2020, there was another substantial increase. To what does the site attribute most of this increase to? Explain what this this type of violation entails.

The 2020 increase is largely due to OCR’s HIPAA Right of Access enforcement initiative, which was launched in late 2019. Since then, OCR has been cracking down on entities that have failed to provide individuals with timely access to their medical records.