|  |  |  |
| --- | --- | --- |
| Security Area | Scenario | Source |
| Information Handling | Ahmad is a medical intern in a medium-sized public hospital where he was recently hired. He has access to the hospital Electronic Medical Records system (EMRs) to perform his duties. To ensure that patient information is preserved securely, the hospital has a firm information privacy policy that any document contains partial or complete information of a patient’s EMR must be kept in secure drawers. Recently, he was contacted by a physician colleague named Emma, who asked Ahmad to access four patient's Electronic Medical Records (EMR) in order to print their medical history including patient's names, medications and diagnoses. Afterwards, she told Ahmad to put those files at the nurses' shared desk in the clinic reception.  Emma’s plan was to collect those files next day afternoon. Thus, Ahmad has expected that printing medications and treatments history and dropping them in the nurses' shared desk would save his colleague’s time. He also knows that printing patient EMR information is a common practice in the hospital and recently an employee was blamed for printing documents, which included sensitive patient information as patient name, diagnosis history, and left them at a shared desk surface. Ahmad printed the requested patients EMR information for Emma and left them at the nurses' shared desk surface in the clinic reception | New Item developed for the Study |
| Social Media Use | Sara is a medical intern in a public large -sized hospital where she has worked for several months, and she has access to the hospital Electronic Medical Records system (EMRs). To ensure that patient information is preserved securely, the hospital has a firm information privacy policy that all medical staff must not share any type or format of information related to patient electronic medical records via the social media websites or applications. One day, Sara was approached by a physician co-worker named Muhammad, who asked her to access a specific patient Electronic Medical Records system (EMRs) and take pictures of the patient EMR screen. Then, sent those pictures back to him via a mobile WhatsApp application, which would give Tony a quick overview of the patient emergency case.  Sara has expected that sending those pictures of the patient information via WhatsApp could save Muhammad's time to deal faster with an emergency case. Although Sara believes sending sensitive patient information via social media application (WhatsApp) may be a violation of the hospital information privacy policy. Sara took several pictures of the patient EMR information screen and shared them with Muhammad via WhatsApp. | New Item developed for the Study |
| Incident Reporting | Ahmad is a physician in a large -sized hospital where is worked for several years. To prevent information privacy breach, the hospital has a firm information privacy policy that is all medical staff must report any security or suspicious activities that may compromise patient information privacy. It includes log-out the hospital's electronic medical records system (EMRs) account if not being used by the authorised person.  Ahmad sees a co-worker physician named Emily, who frequently forgot to log out the hospital's electronic medical record system (EMRs) in her workstation. Emily duties require visiting and examining patients within different clinics. Therefore, expects that Emily is doing that to make her tasks more convenient and to save her time instated of logging in and logging out with every patient request. Ahmad also knows that a physician was reprimanded for leaving his account of the hospital's EMR system opened without physical attendance. Ahmad did not report Emily action to the management and ignored the situation. | New Item developed for the Study |
| Email Use | Antony is a physician in a public hospital where she has worked for few years. However, the hospital has a clear information privacy policy that all medical staff must use the hospital official email and an encryption tool when sending any type of patient information. One day, he wanted a consultation from a physician colleague named Jolly, who had travelled abroad to attend a medical conference. Antony accessed and printed a specific patient's electronic medical records (EMR), scanned it and forwarded it as an unencrypted file to Jolly’s Gmail account.  By doing so, Antony would get a comprehensive medical consultation from Jolly about the patient medical conditions. Thus, he expected that sending the file unencrypted via commercial email will be much faster way to get a response from Jolly. Although Antony believes sending unencrypted sensitive patient information via commercial email may be a violation of the hospital's information privacy policy. Antony moved forwarded and attached an unencrypted patient EMR file and sent it to Jolly's Gmail email account. | New Item developed for the Study |