|  |  |  |
| --- | --- | --- |
| Security Area | Scenario | Source |
| Information Handling | Sara is a pharmacist in a medium-sized hospital where she was recently hired. She has access to the hospital Electronic Medical Records system (EMRs) to perform her 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, she was contacted by physician colleague named Charles, who asked Sara to print medications history for several patients and left them at the nurses' shared reception desk.  Charles’s plan was to collect those files next day morning. Thus, Sara has expected that printing patients’ medications history and dropping them in the nurses' shared reception desk will save her colleague’s time. She also knows that printing patient EMR information is a common practice in the hospital and an employee recently was blamed for printing documents, which included sensitive patient information and left it at a shared desk. Sara printed the requested patients EMR information for Charles and dropped them in the nurses a shared desk. | Adapted from (Siponen & Vance 2010)(Vance et al. 2013) |
| Social Media Use | John is a nurse in a public large -sized hospital where he has worked for several years, and he 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, John is approached by a physician co-worker named Tony, who asked him to access a specific patient electronic medical records (EMR) and take pictures of the EMR screen. Then, send those pictures back to him via a mobile WhatsApp application, which will give Tony a quick overview of the patient emergency case.  John has expected that sending those pictures of the patient EMR via WhatsApp could save Tony's time to deal faster with an emergency case. Although John believes sending sensitive patient information via social media application (WhatsApp) may be a violation of the hospital information privacy policy. John took pictures of the patient EMR information and shared them with Tony via WhatsApp. | Adapted from (Siponen & Vance 2010)(Vance et al. 2013) |
| 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. | Adapted from (Siponen & Vance 2010)(Vance et al. 2013) |
| 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. | Adapted from (Siponen & Vance 2010)(Vance et al. 2013) |