Threat Event	Threat Source	Vulnerabilities	Impact	Asset	Overall Likelihood	Level of Impact	Security Controls
Error in the role assignment leads to elevation of privilege.	Admin	Insufficient routines	Unauthorized data modification	Data integrity	Unlikely	Severe	1. Strengthen routines for access control policy specification. 2. Conduct regular audits of assigned user roles.
Error in the role assignment leads to elevation of privilege.	Admin	Insufficient routines	Unauthorized data access	Data confidentiality	Likely	Severe	1. Strengthen routines for access control policy specification. 2. Conduct regular audits of assigned user roles.
Error in the role assignment leads to elevation of privilege.	Admin	Insufficient routines	Unauthorized data access	Privacy	Likely	Minor	1. Strengthen routines for access control policy specification. 2. Conduct regular audits of assigned user roles.
SQL injection attack leads to successful SQL injection.	Cyber criminal	Insufficient input validation	Unauthorized data modification	Data integrity	Unlikely	Severe	Implement strong input validation.
SQL injection attack leads to successful SQL injection.	Cyber criminal	Insufficient input validation	Unauthorized data access	Data confidentiality	Likely	Severe	Implement strong input validation.
SQL injection attack leads to successful SQL injection.	Cyber criminal	Insufficient input validation	Unauthorized data access	Privacy	Likely	Minor	Implement strong input validation.
Error in assignment of privacy level leads to insufficient data anonymization.	Data reviewer	Insufficient routines	Unauthorized access to personal identifiable information	Data confidentiality	Unlikely	Catastrophic	Strengthen routines for privacy level specification.
Error in assignment of privacy level leads to insufficient data anonymization.	Data reviewer	Insufficient routines	Unauthorized access to personal identifiable information	Privacy	Unlikely	Critical	Strengthen routines for privacy level specification.
Cyber criminal sends crafted phishing emails to HCN users and this leads to sniffing of user credentials.	Cyber criminal	1. Lack of security awareness 2. Weak authentication	Unauthorized access to HCN	Data confidentiality	Very likely	Severe	1. Improve security training. 2. Strengthen authentication mechanism.
Cyber criminal sends crafted phishing emails to HCN users and this leads to sniffing of user credentials.	Cyber criminal	1. Lack of security awareness 2. Weak authentication	Unauthorized access to HCN	Privacy	Very likely	Severe	1. Improve security training. 2. Strengthen authentication mechanism.
Cyber criminal sends crafted phishing emails to HCN users and this leads to that HCN network infected by malware.	Cyber criminal	Lack of security awareness	Leakage of patient data	Privacy	Very unlikely	Critical	Improve security training.
Cyber criminal sends crafted phishing emails to HCN users and this leads to that HCN network infected by malware.	Cyber criminal	Lack of security awareness	Leakage of patient data	Data confidentiality	Very unlikely	Severe	Improve security training.
HCN user connects private mobile device to the network and this leads to that HCN network infected by malware.	HCN user	1. Insufficient security policy 2. Insufficient malware detection	Leakage of patient data	Privacy	Very unlikely	Critical	1. Impose security policy on the use of mobile devices. 2. Implement state-of-the-art malware detection.
HCN user connects private mobile device to the network and this leads to that HCN network infected by malware.	HCN user	1. Insufficient security policy 2. Insufficient malware detection	Leakage of patient data	Data confidentiality	Very unlikely	Severe	1. Impose security policy on the use of mobile devices. 2. Implement state-of-the-art malware detection.