# Comprehensive Report on the Tri-City Healthcare District Cybersecurity Incident

**Executive Summary:** On November 9, 2023, Tri-City Healthcare District, a 388-bed acute-care hospital serving residents in Oceanside, Carlsbad, and Vista within San Diego County, fell victim to a cybersecurity attack by INC Ransom, a relatively new ransomware group. This incident led to significant operational disruptions, including the diversion of emergency patients to neighboring facilities and a temporary halt on all elective procedures. Despite efforts to restore services, the breach resulted in the theft of sensitive data, including patient medical records and financial documents related to the California State Department of Health. This report delves into the incident's details, including the timeline, the response from Tri-City, the nature of the stolen information, and recommendations for future prevention.

**Incident Overview:** The cyberattack was first detected on November 9, 2023, with the hospital promptly taking systems offline to contain the breach. However, emergency services faced disruptions for five days, with emergency patients being diverted and elective procedures postponed. INC Ransom subsequently claimed responsibility for the attack on December 7, 2023, and released a "Proof Pack" of stolen files, showcasing the depth of their access to Tri-City's network.

**Stolen Information:** The stolen data encompassed a wide array of sensitive information, ranging from patient medical records and surgical authorization forms to financial records tied to the California State Department of Health. Particularly alarming was the exposure of the department's bank account number used for fund transfers.

**Hospital Response:** Tri-City engaged third-party cybersecurity specialists and law enforcement to investigate the breach and formulate new prevention strategies. The hospital also worked to restore services, with most operations resuming by November 17. However, there has been no official confirmation regarding the full extent of the data compromised or any misuse of the stolen information.

**Analysis:** The breach underscores the growing threat of ransomware attacks on healthcare institutions, which often target vulnerable systems to extract sensitive data. INC Ransom's use of spear phishing emails and exploitation of the Citrix Bleed vulnerability highlights the sophisticated methods employed by cybercriminals. Moreover, the incident's timing, amidst Tri-City's ongoing partnership with UC San Diego Health, emphasizes the need for enhanced cybersecurity measures in healthcare transitions.

**Recommendations:**

- **Strengthening Cybersecurity Measures:** Immediate actions should include patching vulnerabilities, enhancing network monitoring, and implementing stronger access controls.
- **Employee Training:** Regular training on recognizing phishing attempts and secure data handling practices can mitigate human error, a common entry point for cyberattacks.
- **Incident Response Plan:** Developing and regularly updating a comprehensive incident response plan can ensure a swift and effective reaction to future cyber threats.
- **Community and Patient Communication:** Transparent communication regarding the breach's scope and measures taken to secure data can help rebuild trust with patients and the community.
- **Collaboration with Law Enforcement:** Ongoing cooperation with law enforcement and cybersecurity agencies can facilitate the sharing of threat intelligence and bolster defense mechanisms.

**Conclusion:** The cyberattack on Tri-City Healthcare District highlights the critical importance of robust cybersecurity defenses in protecting patient data and maintaining hospital operations. While the hospital has made efforts to recover from the incident, this event serves as a stark reminder of the relentless threat posed by cybercriminals, particularly against the healthcare sector. Proactive measures, continuous vigilance, and a culture of cybersecurity awareness are essential to safeguard against similar incidents in the future.