Abstract – This document highlights the cyber threats to medical technology and communication technology protocols and outlines the potential risks and vulnerabilities in these systems. It is designed to help healthcare organizations and medical professionals understand the importance of securing their technology systems to protect patient data and ensure the continuity of care.

I. Introduction

The integration of Internet of Things (IoT) devices in the healthcare and public health sectors has brought about significant advancements in patient care and operational efficiency. However, these benefits come with a set of cybersecurity challenges and threats that need to be addressed to protect sensitive health information and ensure the continuity of healthcare services. Here's a comprehensive overview of the cybersecurity threats in these sectors, focusing on devices like pacemakers, smart infusion pumps, MRI machines, and the broader implications for medical technology and communication protocols.

The security of digital technologies in the healthcare and public health sector is paramount for protecting patient safety, privacy, and the integrity of medical services. Healthcare organizations must adopt a comprehensive approach to data security, network security, and device security, implementing encryption, secure communication protocols, and robust network and device security measures. Compliance with HIPAA regulations and adherence to best practices and standards, such as those provided by CISA, HHS, and DICOM, are essential for mitigating cyber threats and ensuring the secure use of digital technologies in healthcare

II. Industries

Cyber attacks on medical technology can affect a wide range of industries beyond the immediate healthcare sector. The ripple effects of a cyber attack on medical technology can extend far beyond the immediate healthcare sector, impacting a wide array of industries and services that are interconnected with healthcare delivery and operations.

The affected industries include:

- **Healthcare Providers**: Hospitals, clinics, and private practices rely on medical technology for patient care. Cyber attacks can disrupt clinical operations, delay treatments, and compromise patient safety.
- **Healthcare Technology Companies**: Firms that develop and maintain medical software and devices can suffer from intellectual property theft, loss of customer trust, and financial losses due to cyber attacks.
- **Insurance Companies**: Insurers may face claims related to cyber attacks on medical technology, including costs associated with data breaches, system restoration, and liability claims.
- **Pharmaceuticals and Biotech**: These industries rely on medical data for research and development. Cyber attacks can lead to the loss of proprietary research data and disrupt the supply chain for critical medications.
- **Healthcare IT Services**: Companies providing IT support and services to healthcare organizations can be indirectly affected by cyber attacks on their clients, leading to reputational damage and financial losses.
- **Government and Regulatory Bodies**: Government health agencies and regulatory bodies may need to respond to cyber attacks on medical technology, affecting public health and potentially leading to regulatory changes.
- **Emergency Services**: Cyber attacks that disrupt medical technology can lead to delays in emergency response and patient transfers, affecting ambulance services and emergency medical care
- **Legal and Compliance Services**: Law firms and compliance consultants may see an increase in demand for their services as healthcare organizations navigate the legal ramifications of cyber attacks.
- **Cybersecurity Firms**: These attacks can lead to increased demand for cybersecurity services, as healthcare organizations seek to bolster their defenses against future incidents.
- **Patients and the Public**: Ultimately, the public is affected as patients may experience compromised care, privacy breaches, and a loss of confidence in the healthcare system.

III. General Vulnerabilities and Threats

The healthcare and public health sector is increasingly reliant on digital technologies for managing patient information, medical procedures, and communication. This digital transformation, while beneficial, introduces significant security risks, including data breaches, unauthorized access, and cyberattacks, which can compromise patient safety, privacy, and the integrity of medical services

Common cyber threats to medical technology and communication technology protocols include disruption, degradation, and destruction of devices, data poisoning, theft of personal and proprietary data, and unauthorized access to medical software. These threats are exacerbated by the expansion of the interoperable IT/OT environment in healthcare, the use of artificial intelligence (AI) and machine learning (ML)-

enabled medical devices, and the increasing reliance on wireless connectivity, including 5G.

Medical devices, such as pacemakers, smart infusion pumps, and MRI machines, may be vulnerable to cyber incidents due to lack of data encryption protocols, poor network segmentation, and unpatched vulnerabilities. Additionally, medical software, such as DICOM and PACS, may lack proper input validation, transmit data in cleartext, and use poor cryptographic algorithms, making them susceptible to unauthorized access and data modification.

A. Smart Infusion Pumps:

These devices connect to hospital internal networks via Wi-Fi or Ethernet and transmit status, alerts, and alarms to central monitoring/control stations, as well as transfer data to Electronic Health Records (EHR).

B. MRI Machines:

MRI machines may be connected to the hospital's internal network, and scans can be encoded and sent to Picture Archiving and Communication System (PACS) software via Digital Imaging and Communications in Medicine (DICOM). PACS images may be stored locally and made available on web-based EHR, potentially allowing unauthorized access to clinicians on network devices, including computers.

C. Pacemakers:

Pacemakers and other cardiac implantable electronic devices (CIEDs) have evolved to include wireless connectivity for monitoring and programming. This connectivity, while beneficial for patient care, introduces vulnerabilities. Cyberattacks could potentially lead to device malfunction or unauthorized access to patient data, posing significant risks to patient health

D. IoT Devices:

Many IoT devices in healthcare lack robust security controls, making them susceptible to unauthorized access and data breaches. This includes issues with data encryption, cleartext data transmission, and insecure storage of passwords.

E. Third-Party Vendors:

Devices and software provided by third-party vendors can introduce vulnerabilities into healthcare networks, offering a backdoor for cyberattacks.

F. Medical Software:

Software like DICOM and PACS may lack proper input validation and use insecure communication protocols, increasing the risk of unauthorized access and data manipulation.

G. Radio Frequency (RF) Interference:

RF interference can disrupt device communication, leading to data loss or misinterpretation, which can have direct implications on patient care.

H. 5G Connectivity:

The adoption of 5G technology in healthcare introduces new vulnerabilities through expanded attack surfaces and potential supply chain risks.

IV. Addressing Risks

Addressing these risks requires a comprehensive approach to data security, network security, and device security.

A. Data Security

Data security in healthcare involves protecting sensitive patient information from unauthorized access, disclosure, and theft. The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for protecting patient data, requiring encryption of electronic Protected Health Information (ePHI), unique user identification, and audit trails to monitor access and usage of PHI. Encryption is a critical technology for securing data during transfer, use, and storage, ensuring that data is unreadable to unauthorized individuals. Additionally, the adoption of secure communication protocols, such as those outlined by DICOM for medical data transfer, is essential for maintaining the confidentiality and integrity of patient information.

B. Network Security

Network security in the healthcare sector involves protecting the infrastructure that supports the transmission and storage of medical data. This includes securing wireless networks, implementing firewalls, and using virtual private networks (VPNs) to encrypt data in transit. The Cybersecurity and Infrastructure Security Agency (CISA) provides resources and best practices for strengthening network defenses and mitigating cyber threats. Healthcare organizations must also ensure that their network security measures comply with HIPAA regulations and other relevant standards.

C. Device Security

Device security focuses on protecting medical devices and mobile devices used in healthcare settings from cyber threats. This includes implementing strong authentication mechanisms, encrypting data stored on devices, and regularly updating device software to address security vulnerabilities. The increasing use of Internet of Medical Things (IoMT) devices introduces additional security challenges, requiring healthcare organizations to adopt comprehensive security measures to protect these devices from hacking and unauthorized access

V. Attack Consequences

The consequences of a Cyber attack on medical technology can be severe and wide-ranging, affecting patients, healthcare organizations, and medical device manufacturers.

- **Compromised patient safety**: Cyber attacks on medical devices, such as pacemakers, smart infusion pumps, or MRI machines, can lead to disruption, degradation, or destruction of these devices, potentially endangering patient health and even lives.
- **Loss of sensitive data**: Hackers may steal or expose sensitive patient data, including personal information, treatment records, and financial statements, leading to privacy breaches and potential identity theft.
- **Financial and legal penalties**: Healthcare organizations may face significant fines, legal consequences, and sanctions for failing to secure patient data properly and comply with regulations like HIPAA.

- **Reputational damage**: Cyber attacks can erode patient trust and damage the reputation of healthcare organizations and medical device manufacturers, which can be difficult to recover from.
- **Operational disruptions**: Cyber incidents can cause prolonged IT or production failures, paralyzing critical healthcare services and threatening the existence of affected organizations.
- **Hindered innovation**: The persistent threat of Cyber attacks may limit the adoption of new technologies and slow down innovation in the healthcare sector

A. Smart Infusion Pumps

The consequences of a Cyber attack on smart infusion pumps can be severe and potentially life-threatening. Smart infusion pumps are network-connected devices that deliver medications and fluids to patients, and they are commonly used in hospitals and clinics. According to a study by Palo Alto Networks' Unit 42 threat research service, 75% of infusion pumps have cybersecurity flaws, putting them at increased risk of being compromised by hackers

These cybersecurity flaws can lead to various consequences, including:

- **Unauthorized access**: Hackers can gain unauthorized access to infusion pumps, potentially allowing them to change how the pump delivers intravenous medications. This can result in patients receiving incorrect dosages, which can be harmful or even fatal.
- **Interception of unencrypted communications**: Some infusion pumps transmit unencrypted communications, which can be intercepted by hackers. This can lead to the exposure of sensitive patient data, such as medical records and personal information.
- **Exploitation of known vulnerabilities**: Infusion pumps may have known security gaps, such as leaving usernames and passwords unchanged from the device's default factory settings. These vulnerabilities can be easily exploited by hackers, potentially putting patients at risk or exposing private data.
- **Disruption of services**: disrupt healthcare services, leading to software outages, loss of access to health records, and inability to provide appropriate care. In extreme cases, healthcare facilities may be forced to divert patients to other medical centers or cancel surgeries.

B. MIR Machines

The consequences of a Cyber attack on MRI machines are multifaceted and can significantly impact patient safety, data integrity, and healthcare operations.

- **Patient Safety Risks**: Cyber attacks can lead to the manipulation of MRI images, potentially resulting in incorrect diagnoses. For instance, attackers could alter images to either remove a tumor or erroneously add one, leading to misdiagnosis and inappropriate treatment, which could be fatal.
- **Disruption of Healthcare Services**: MRI machines are crucial for diagnosing and monitoring various conditions. A Cyber attack could disable these machines, causing delays in diagnosis and treatment. In critical situations, even small delays can have severe consequences for patient health.
- **Ransomware Attacks**: MRI machines, like other medical devices, are vulnerable to ransomware attacks. Such attacks could block access to the machines or encrypt the images, demanding a ransom to restore access. This not only disrupts healthcare services but also puts patient data at risk.
- **Exposure of Sensitive Data**: MRI machines are connected to hospital networks, making them potential entry points for attackers to access and steal sensitive patient data, including personal and health information. This breach of privacy can have legal and financial implications for healthcare providers.
- **Operational and Financial Impact**: Recovering from a Cyber attack on MRI machines can be costly and time-consuming. Healthcare providers may need to replace or repair compromised devices, and face potential legal penalties and loss of trust from patients.
- **Regulatory Challenges**: Strict regulations make it difficult to conduct basic updates on medical PCs connected to MRI machines, complicating efforts to protect against Cyber attacks. The slow development process of medical imaging devices also leaves them vulnerable to evolving cyber threats

C. Pacemakers

The consequences of a Cyber attack on pacemakers can be severe and potentially life-threatening. Cybersecurity vulnerabilities in pacemakers were first exposed by hackers in 2011, and since then, various security flaws have been discovered. In 2017, the US Food and Drug Administration (FDA) recalled an implantable pacemaker due to concerns that it could be hacked

Potential consequences of a on pacemakers include:

- **Direct Threat to Patient Life**: can lead to life-threatening situations. Attackers could potentially take control of the device, altering pacing functions or delivering inappropriate electrical shocks, which could result in severe health complications or even death.
- **Battery Drainage**: Certain types of attacks, such as those involving the continuous sending of commands to the pacemaker, could lead to rapid battery depletion. This would necessitate an early surgical intervention to replace the device, posing additional health risks to the patient.
- **Unauthorized Access to Personal and Medical Data**: Pacemakers can store and transmit data regarding patient health and device performance. Cyber attacks could compromise the confidentiality of this data, leading to privacy breaches and potential misuse of personal information.
- **Loss of Confidence in Medical Devices**: Widespread knowledge of vulnerabilities and successful attacks

could erode public trust in pacemakers and other medical devices. This loss of confidence could deter patients from opting for potentially life-saving treatments

D. Medical IoTs

Cyber attacks on IoT medical devices can have severe consequences for patient care, including loss of life. The primary target for cyber attackers are Internet of Things (IoT) and Internet of Medical Things (IoMT) devices, which were the root cause for 21% of all ransomware attacks in the healthcare industry. The top-10 bedside devices that pose the greatest security risks include infusion pumps, VoIP devices, ultrasound machines, patient monitors, and medicine dispensers.

- **Patient Safety Risks**: can directly threaten patient lives by compromising the functionality of medical IoT devices such as pacemakers, insulin pumps, and ventilators. For example, attackers could alter device settings or functionality, leading to inappropriate treatment or device failure.
- **Data Breaches**: IoT medical devices often collect and transmit sensitive patient data. Cyber attacks can lead to unauthorized access to this data, resulting in privacy violations, identity theft, and potential misuse of personal health information.
- **Operational Disruptions**: can disrupt healthcare operations by disabling medical devices, leading to delays in diagnosis, treatment, and care delivery. This can have cascading effects on patient flow and hospital capacity.
- **Financial Costs**: The aftermath of a can impose significant financial burdens on healthcare organizations, including costs associated with device replacement or repair, data breach response, increased insurance premiums, and potential legal liabilities.
- **Loss of Trust**: can erode trust between patients and healthcare providers. Patients may become hesitant to use certain medical devices or share their data, fearing privacy breaches and questioning the reliability of their care.
- **Regulatory and Legal Implications**: Healthcare organizations may face regulatory penalties for failing to protect patient data and ensure the security of medical devices. Legal actions could also arise from affected patients or regulatory bodies.
- **National Security** Threats: In the context of defense and military operations, compromised IoT devices could reveal sensitive information, posing national security risks. Third-Party Vendors

E. Third-party vendors

Cyber attacks on third-party vendors in the medical sector can have severe consequences for both the healthcare organizations and the patients they serve. These attacks pose one of the biggest challenges on the healthcare cyber-risk landscape, with hospitals and health systems at increasing risk of cyberattacks on third parties such as business associates, medical device providers, and supply chain vendors. These consequences include:

- **Data Breach**: Third-party vendors often have access to sensitive data. If a third-party vendor is hacked, this data could be compromised, leading to unauthorized access to patient information and financial data.
- **Malware Infections**: If a third-party vendor's system is infected with malware, it could spread to your organization's system through the vendor.
- **Ransomware Attacks**: Many ransomware attacks occur through third-party vendors. If these vendors lack robust security and cyber defense measures, they can become an entry point for ransomware attacks.
- **Distributed Denial of Services (DDoS) Attacks**: Your organization could be targeted by DDoS attacks through third-party vendor systems.
- **Compliance Failures**: Third-party vendors may not always comply with the same regulations as the organizations they work with. This could lead to compliance failures for the organizations.
- **Reputation Damage**: If a third-party vendor is hacked, it could damage the reputation of the organizations they work with.
- **Impact on Medical Devices**: Cyber attacks on third-party vendors can potentially affect medical devices such as CT and MRI machines, which are commonly connected to hospital networks. Vulnerabilities in outdated firmware can be exploited by cyber attackers, disrupting digital patient records and potentially jeopardizing patients' health

F. Medical Software

The consequences of a cyber attack on medical software are significant and multifaceted, impacting not only the healthcare organizations but also the patients they serve. The consequences of a cyber attack on medical software extend beyond immediate financial losses, posing serious risks to patient safety, data integrity, and the overall effectiveness of healthcare delivery. It underscores the importance of prioritizing cybersecurity measures to protect sensitive health information and ensure the continuity and quality of care

- **Data Breaches**: can lead to unauthorized access to sensitive patient data, including personal and financial information, medical records, and treatment histories. This compromises patient privacy and can result in identity theft and financial fraud.
- **Financial and Legal Penalties**: Healthcare organizations may face substantial financial losses due to fines and legal penalties for failing to protect patient data adequately. The costs associated with responding to a breach, such as notification expenses and credit monitoring services for affected individuals
- **Patient Safety Concerns**: can disrupt healthcare services and compromise patient safety. For example, tampering with medical records or diagnostic software could lead to incorrect diagnoses, inappropriate treatments, or delays in care.

- **Damage to Patient Trust and Reputation**: erode trust between patients and healthcare providers. Patients may lose confidence in an organization's ability to protect their data and provide safe care, damaging the organization's reputation and potentially leading to a loss of business.
- **Loss of Productivity**: can disrupt healthcare operations, leading to delays in procedures and tests, longer patient stays, and overall reduced efficiency. This can strain healthcare resources and negatively impact patient care.
- **Increased Mortality Rates**: In some cases, cyber attacks have been linked to increased patient mortality rates. Delays in procedures, tests, and the provision of care due to cyber incidents can have dire consequences for patient outcomes.
- **Compromised Value-Based Models**: can undermine the efforts of healthcare organizations to deliver value-based care by compromising the quality and integrity of data, which is crucial for making informed decisions about patient care.
- **Limited Innovation**: Persistent and large-scale cyber attacks can stifle innovation within the healthcare sector. Concerns about cybersecurity may deter organizations from adopting new technologies that could improve patient care and operational efficiency.

G. Radio Frequency (RF) Interference medical

The consequences on Radio Frequency (RF) Interference in the medical field can be severe, as it can compromise the functionality and security of medical devices that rely on RF communication.

- **Interference with Device Functionality**: can disrupt the normal operation of medical devices, potentially leading to incorrect readings or malfunctions. This can have serious consequences for patient care, especially in critical situations where accurate measurements and device performance are essential.
- **Data Breaches**: RF interference can potentially be exploited to gain unauthorized access to sensitive patient data transmitted through RF communication channels. This can lead to data breaches, exposing personal and medical information, and potentially compromising patient privacy.
- **Device Tampering**: could potentially manipulate RF signals to send unauthorized commands to medical devices, such as pacemakers or insulin pumps, potentially causing harm to patients. This can include altering device settings, administering incorrect dosages, or even shutting down devices entirely.
- **Denial of Service**: can cause devices to become unresponsive or malfunction, leading to a denial of service. This can disrupt patient care and potentially put patients at risk, especially in situations where immediate medical attention is required.
- **Loss of Trust: Successful** attacks on RF interference can erode public trust in medical devices and the healthcare system as a whole, potentially leading to a reluctance to use such devices or seek medical care.

H. 5G Connectivity

The consequences on 5G connectivity in the medical field can be substantial, given the critical role of 5G in enhancing communication and data transfer within healthcare systems:

- **Increased Attack Surfaces**: The expansion of 5G networks increases the number of potential entry points for cyber attackers, making it more challenging to secure the network against unauthorized access and data breaches.
- **Vulnerabilities in IoT Devices**: medical devices are part of the Internet of Medical Things (IoMT) and rely on 5G for connectivity. These devices may have inherent security weaknesses that can be exploited, leading to compromised patient data and device functionality.
- **GPRS Tunneling Protocol Risks**: The use of GPRS tunneling protocols in 5G networks can introduce security vulnerabilities, potentially allowing attackers to intercept and manipulate transmitted data.
- **Legacy Network Connections**: 5G networks connected to legacy systems may inherit existing vulnerabilities, providing cyber attackers with opportunities to exploit these weaknesses and gain access to sensitive medical data and systems.
- **Increased Bandwidth Challenges**: The higher bandwidth of 5G networks can strain current security monitoring capabilities, making it more difficult to detect and respond to threats in real-time.
- **Network Function Virtualization**: The reliance on software and virtualization in 5G networks introduces new security challenges, as each virtual component needs to be monitored and secured to prevent potential breaches.
- **IMSI Encryption** Weaknesses: Weaknesses in IMSI encryption can lead to vulnerabilities in subscriber identity confidentiality, potentially allowing man-in-the-middle attacks and unauthorized tracking of devices.
- **Botnet and DDoS Attacks**: The increased number of connected devices in a 5G network can be leveraged by attackers to create botnets or launch distributed denial-of-service (DDoS) attacks, which can disrupt medical services and data availability.
- **Disruption of Critical Healthcare Services**: Cyber attacks on 5G networks can disrupt the communication between medical devices and healthcare providers, leading to delays in critical care and potentially endangering patient lives.
- **Regulatory and Compliance Implications**: Healthcare organizations may face regulatory scrutiny and penalties if they fail to protect patient data and ensure the security of their 5G-enabled medical devices and services