A recent cybersecurity data breach at the Department of Veteran Affairs (VA) has potentially exposed the personal information of 46,000 veterans. This recent cyber data breach involved an online software application that handled medical payments. Likewise, the Defense Health Agency (DHA) experienced a massive cyber data breach earlier this year involving over 1.1 billion medical records and the patient data of servicemembers including X-Rays, MRIs and other health data. Security research firm Comparitech counted 443 cyber data breaches among U.S. government agencies and military branches between 2014-2018. According to the American Medical Association (AMA), in just the past 12 months, 39.9 million U.S. health care records have been reported as breached by the U.S. health care industry.

It is essential that the U.S. public and private health care sectors work together to ensure that U.S. citizens are protected from health care cyberattacks and data breaches. Cyber data breaches in the health care ecosystem can result in the theft of:

- Personal identifiable information (PII)
- Protected health information (PHI)
- Electronic health records (EHR)
- Medical images, payment card information (PCI)
- Health-related research and development (R&D) intellectual property (IP)

Plus, cyberattacks can result in the disruption of patient services and medical treatments and even the loss of human life. This white paper is focused on increasing awareness of the cyber and data privacy threats and cyberattack trends facing the public and private sectors of the U.S. health care ecosystem. The paper also offers proven cybersecurity best practices.

**Tremendous growth of ransomware cyberattacks**

Ransomware attacks are a prominent part of the cyber threat landscape for the U.S. health care ecosystem. This year has been a banner year with a 650%+ increase in ransomware attacks in the United States, according to Cisco—especially the use of Ryuk ransomware, Robbinhood ransomware and SamSam ransomware. Most of the cyberattack campaigns on the U.S. health care public sector have used massive phishing or exploit kit techniques to widely distribute ransomware and achieve the highest infection rate. Such campaigns often use generic phishing emails with content referring to an invoice, a transaction or a contract. The ransomware distributed in these massive attack campaigns is rarely custom made—in most cases, it is a ransomware file that was purchased in underground forums for several hundred dollars or for a share of the profit. In 2015, the average cyber ransom demand was $25,000, typically requested in the form of a cryptocurrency. According to Cybersecurity Ventures, the average cyber ransom demand today is nearly $200,000 via bitcoin payment or other cryptocurrency.
Significant database misconfiguration—exposing public sector health information

It can almost be taken for granted, that most public health care records and medical documents are uploaded to online servers, so they can be shared in real time with patients, doctors and other health care providers. Collaboration between U.S. federal and state government health agencies, hospitals and medical institutions is leading to the integration of large-scale medical information via joint servers using cloud-based services such as Amazon Web Services (AWS).

While data sharing and integration can lead to better preventative care, preparation for wider medical trends and further study of new and known diseases, it can and does also lead to various forms of software misconfigurations and system integration issues, which can lead to potential loss, damage or theft of medical data.

Legacy systems and unpatched software present real and present danger

Up-to-date and fully patched operating systems and software are fundamental security measures, especially for the data storage and collection environments of public sector health agencies. Running a legacy operating system, especially those that have been unsupported for five years or longer, greatly increases the risk of a breach.

Because many public health care institutions are faced with significant budget challenges, security procedures can fall behind in priority. Additionally, many veteran health care employees prefer using familiar, older and simpler consumer machines to support their day-to-day practice. This means that many U.S. public health care organizations are vulnerable to cyberattacks that use known exploits. In such cases, an attacker can bypass the need for any special preparations to access a medical database or a health care facility's network—one unpatched server in the network is all that is required.

The rise of spear-phishing attacks in the U.S. health care ecosystem

While spear-phishing email cyberattacks are a dominant threat for almost all industries, these cyberattacks are especially applicable to the U.S. health care sector. Phishing is the main method attackers employ to initiate attacks for planting malware or stealing PHI. A cybersecurity report published by the Healthcare Information and Management Systems Society (HIMSS) in 2019 listed phishing as the most commonly used method for initiating attacks in the health sector. Moreover, a survey conducted by the Journal of the American Medical Association (JAMA) Network in March 2019 found that the click rate of phishing emails within the health care industry was 16.7%.

Health care systems are also uniquely vulnerable to phishing attacks. Employee turnover at hospitals is high and there is a constant influx of new employees, including interns and students, who may have no prior cybersecurity training. Providing training to every employee who uses a U.S. federal or state government health agency network would require a vast framework and a substantial budget. In addition, hospitals and health care facilities are vulnerable through their large number of Internet of Things (IoT) devices as well as employee smartphones connected to the network.

IoT medical device security is essential

IoT systems are considered one of the weakest network components. These connected devices often use a custom-developed software adapted to a specific operating system (OS) version and updated in long time intervals—forcing them to often rely on outdated software and legacy operating systems that leave them vulnerable to attacks. IoT devices are also increasingly collecting and storing vast amounts of unique data, which make them an attractive target for cyber criminals. Lastly, IoT devices may serve as an easy entry point to a network.

The U.S. health care ecosystem, in both the public and private sector, has seen a particularly sharp increase in the use of IoT devices, driven partly by the rise in wearables and remote patient monitoring. Clinical uses of IoT have expanded as well, and the average hospital room now contains an estimated 15-20 connected medical devices. A large Veteran Affairs (VA) hospital could have as many as 85,000 connected devices and that number will only continue to rise in coming years.

While these IoT devices can have a role in improving efficiencies and the delivery of care, they also increase vulnerability to cyber-attacks. Another difficulty lies in the remediation of an infected IoT device after an attack has been detected. To remove malware from a medical device, the device must often have all of its software reloaded by the manufacturer itself. If a vulnerability has been uncovered, the same goes for all of those devices in use around the world. Hospital staff are not equipped or able to access the core of IoT medical devices approved by the U.S. Food and Drug Administration (FDA)—they cannot address security incidents in IoT devices on their own.

2 https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2727270
Perspecta top ten cybersecurity recommendations

Based upon our extensive experience consulting with U.S. federal, state and local government health agencies nationwide and serving as a leading technology systems integrator, we offer the following cybersecurity recommendations for consideration by government health care agencies:

1. **Develop and implement a threat-based cybersecurity (TBC) methodology:** A proactive approach to identify high-value data, assess data storage and transmission for vulnerabilities and mitigate the most likely risks and attack vectors. This maximizes the efficacy of cybersecurity resources by focusing on an organization’s unique threat profile. Achieving this comes as part of a continuous process that responds to emerging cyber threats.

2. **Transition to cybersecurity managed services:** Government agencies are increasingly realizing the value of outsourcing cybersecurity services to experienced system integrators and managed security service providers to deliver technologies and tools that increase the use of data automation, workflow automation, big-data analytics and data visualization to drive enhanced performance and cost-effectiveness. Moving from a cybersecurity contractor staff augmentation business model to a cybersecurity managed services model requires planning to select the right performance measures and metrics and ensure a smooth transition. Typical cybersecurity managed services include:
   - Security operation centers (SOC) services
   - Security information and event management (SIEM) services
   - Incident response management (IRM)
   - Vulnerability management
   - Cyber threat intelligence (CTI)

3. **Enhance identity, credential and access management (ICAM) across the enterprise:** develop technical policies and procedures to ensure that only authorized employees have access to PHI, EHR, medical images and PII. Then, implement an enterprise-wide end-to-end ICAM software with multifactor authentication (MFA) and credential-based boundaries or role-based boundaries.

4. **Use a cyber range and cyber exercises to educate and train health care professionals:** leverage the capabilities of a cloud-based cyber range with emulated health care information systems and simulated cyberattacks to provide persistent cyber education and training for health care IT professionals combined with tabletop exercises for health care leadership.

5. **Create a “zero trust” (ZT) data environment:** build a zero trust environment including policies, plans and a zero trust architecture (ZTA), including data micro-segmentation, micro-perimeters, data segmentation gateways and ICAM to the borders.

6. **Implement an AI-driven intrusion detection system (IDS):** implement new software using AI and machine learning (ML) capabilities to more accurately monitor traffic moving throughout email, network and information system endpoints to identify suspicious activity and clear threats in real-time.

7. **Develop and test an internal and external cyber data breach communications plan:** align with existing enterprise risk management frameworks (i.e., HIPAA, HITRUST- CSF, NIST SP 800-37 and NIST SP 800-53).

8. **Implement and test a cyber incident response plan:** include the participation of organization leadership and key personnel from all technology, business, administration and clinical functions.

9. **Build an insider threat program:** include policies, education, training and the implementation of ZTA to create micro-perimeters and data segmentation that restricts internal vertical and lateral movement within an information system to individuals with approved access.

10. **Establish and test a business continuity plan (BCP):** an effective information back-up capability is vital for real information resilience.

**Summary**

U.S. federal, state and local government health agencies are investing billions of taxpayer dollars in digital transformation projects to leverage emerging technologies—cloud computing, big data analytics, data automation and AI and robotic process automation—with the intent to enhance patient services, increase data analysis and reduce operational costs. These emerging information technologies offer the potential for significant data-centric solutions to various health care related business and operational challenges. Likewise, each technology creates new cybersecurity risks and cyber vulnerabilities to potential data breaches, which can in turn jeopardize data privacy, data security and patient care. Thus, it is essential for U.S. federal, state and local government agencies to implement proven cybersecurity best practices as an integral part of digital transformation planning and implementation efforts to ensure data privacy, data resilience and patient care.