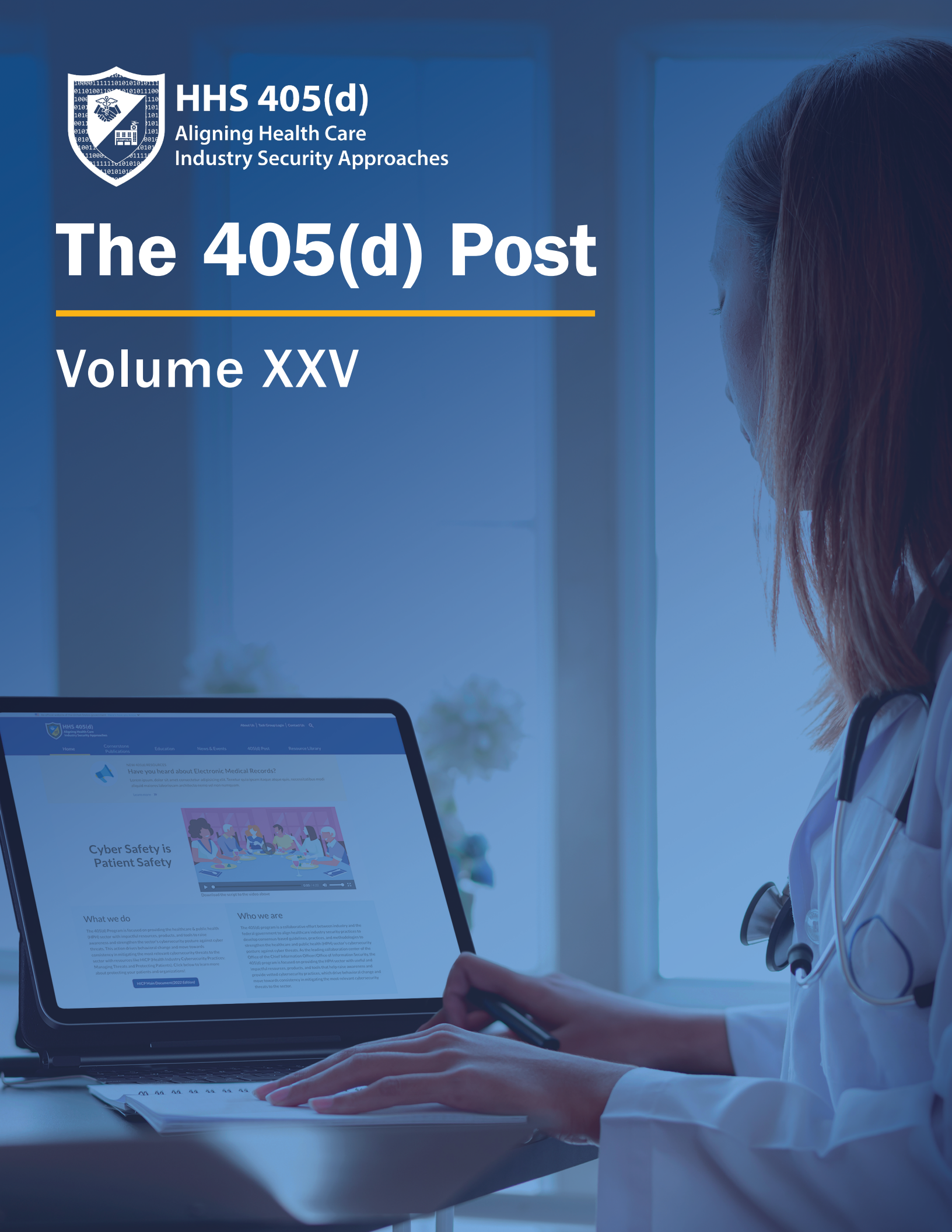
HHS 405(d)
Aligning Health Care
Industry Security Approaches

The 405(d) Post

Volume XXV



A Word from the Task Group

Do You Know The Risk?: The Urgent Need for Data Security in Healthcare AI

By Donna Grindle, 405(d) Task Group Ambassador Lead

In the face of evolving cyber threats, the healthcare sector stands at a pivotal juncture. In the dynamic and fast-paced world of healthcare, embracing the use of Artificial Intelligence (AI) marks a pioneering shift towards enhanced patient care and streamlined operations. AI's potential to deliver personalized treatments and leverage predictive analytics is not just transformative; it's revolutionary. With healthcare institutions relying more on AI to enhance patient care and operational efficiency, the need for robust data protection measures is becoming increasingly crucial. It is essential to create and consistently enforce protocols for assessing data privacy and security issues when choosing and implementing AI technologies as we go, not as an afterthought. Surprisingly, many current AI applications may not have undergone a comprehensive, if any, security evaluation, highlighting the need to address this gap quickly.

The undeniable appeal of artificial intelligence lies in its wide range of benefits, spanning from predictive analytics to tailored treatment strategies. Beyond the patient care applications, the potential for its use to streamline and improve healthcare operations is equally exciting. Yet, amidst this excitement for these innovations, the potential risks are sometimes overlooked. Issues concerning data security and ethical decision-making are significant, since unauthorized use of patient information and biased or poisoned data used in these AI algorithms can lead to ethical quandaries and substantial legal and financial consequences. Neglecting cybersecurity measures goes beyond mere business repercussions. It can undermine the trust we rely on between patients and healthcare providers to provide effective patient care and protect patient safety.

It is essential for organizations to create a detailed blueprint now to seamlessly and securely incorporate AI into various aspects of healthcare, including patient care, cybersecurity, business operations, research and development, finances, and human resources. Such integration is crucial for the present and future of all entities in the sector. Establishing thorough guidelines and protocols will enable organizations to responsibly and effectively utilize AI tools, ultimately improving healthcare services and operational productivity while protecting confidential data and patient safety. Of course, this plan must be expected to constantly evolve as innovation provides more exciting opportunities that are also accompanied by additional risk concerns.

The rate of advancement and investment in AI technologies heightens the importance of creating and following your established guidelines as soon as possible. If you don't have one already, don't delay. You probably have some types of AI technologies already in use within your ecosystem. Your vendors may even be providing them as a new feature that your users have already embraced. Here are a few points to consider including in your AI management plan.

Considerations for your blueprint:

Ethical Framework and Governance

- Establish a governance structure for AI oversight.
- Consider input from all areas of the organization including legal, financials, HR, business operations, IT, cybersecurity, vendors as well as all clinical positions and even patients.
- Prioritize the transparency of AI systems to stakeholders.
- Ensure AI decision-making processes are explainable and understandable.
- Define clearly what your organization determines will fall under your definition of artificial intelligence technologies and their use.
- Require evaluation, similar to new solutions, of AI tools added as a new "feature" for currently implemented technology.
- Define a non-negotiable line for approval requirements for AI implementation, not only by staff but also by vendors, that will be used to access your systems and data. For example, new AI cybersecurity tools or revenue cycle data analysis.
- Define clear lines on the use of generative AI tools such as ChatGPT for use in any job role for any reason.
- Document AI use decisions and reasoning along with those providing input. This information is often needed much later when someone asks "Why are we doing this?"

Education

- Educate your team in charge of making these plans on how to define and recognize the different types of AI technologies, their advantages and the risks they bring to your organization.
- Train all staff, and vendors if needed, to recognize when they are considering or using artificial intelligence technologies.
- Train all staff and vendors on your policies and procedures and the potential pitfalls that come with the wonderful advances AI brings to your ability to deliver care and services.
- Document the training done in all cases as you would other security awareness training including date, time, attendees, and content.

Risk Evaluation

- Assess all potential legal and regulatory risks associated with AI that will be allowed under governance definitions.
- Review and adjust Business Associate Agreements (BAAs) for AI data handling.
- Implement data privacy and security protocols specifically associated with AI tools.
- Develop a custom security risk analysis and assessment for use with AI applications.
- Ensure compliance with regulations as they continue to evolve to address AI.
- Document every review, what was considered and who was involved.
- Document regular reviews of your AI risk management plans which may need to be more frequent than the overall risk management plans due to constant changing opportunities.

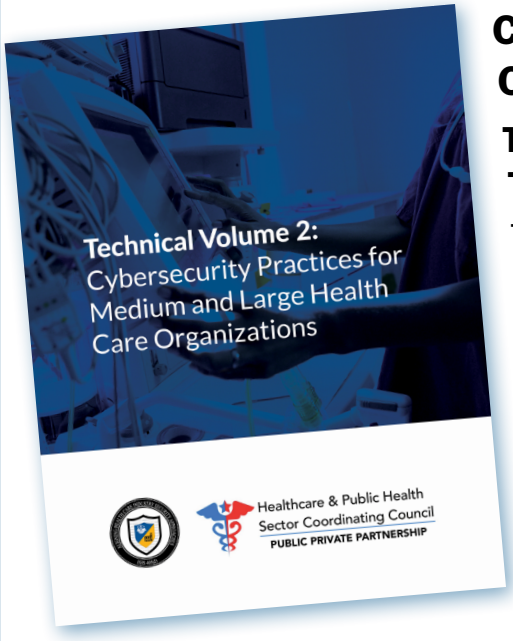
Ongoing Monitoring & Evaluation

- Regularly monitor the use of new AI tools that have not been previously evaluated or have not been clearly defined for acceptable use.
- Regularly monitor for unapproved use of AI technologies.
- Regularly review AI tools for new features, ongoing performance and compliance with standards.
- Adjust AI usage protocols based on evolving challenges and technologies with input from defined roles in the organization.
- Document this activity and findings for your records and future reference.

The rapid deployment of AI in healthcare is a testament to the sector's innovation and commitment to improving patient safety and care. However, the integration of these technologies cannot be at the expense of cybersecurity and ethical integrity. As large enterprises along with small and medium businesses explore AI solutions, it is imperative to incorporate cybersecurity reviews into the planning phase. By doing so, we can safeguard sensitive information, ensure regulatory compliance, and uphold the trust that is fundamental to patient safety and care.

When we hear terms like "Copernican revolution" used in reference to the transformative impact AI will have on healthcare, it certainly captures the magnitude of change we anticipate. We should not allow our enthusiasm to overshadow the ultimate goal of improving patient safety and care through the secure and safe use of these new technologies. All of our actions, or inactions, in this moment can have lasting consequences to real people. Building a strategic plan now will allow organizations to embrace the moment but also remember such a paradigm shift always comes with risks that must be addressed along the way.

HICP in the Spotlight



Cybersecurity Practice 9: Safeguarding Network Connected Medical Devices in Healthcare

The Health Industry Cybersecurity Practices (2023 Edition), Technical Volume 2

The increasing reliance on network-connected medical devices in healthcare has brought significant advancements in patient care but also introduced new cybersecurity risks. These devices, ranging from simple monitors to complex infusion pumps, are essential for diagnosis and treatment. However, their integration into healthcare networks exposes them to cyber threats that can compromise patient safety, data integrity, and overall healthcare delivery. This article discusses the risks posed by these devices and offers tips on how to protect them from cyber threats.

Risks Posed by Network Connected Medical Devices

Patient Safety: One of the most severe risks of compromised medical devices is the potential harm to patients. Devices like infusion pumps and defibrillators, if hacked, can be manipulated to deliver incorrect doses or shocks, leading to potential fatal consequences. For example, a compromised CT scanner could delay the diagnosis and treatment of stroke patients, leading to severe brain damage or death.

Data Integrity and Privacy: Medical devices often store and transmit sensitive patient data, including protected health information (PHI) and personally identifiable information (PII). A breach can lead to unauthorized access to this data, resulting in identity theft and violations of privacy regulations such as HIPAA .

Device Exploitation: Medical devices can be used as entry points for broader network attacks. Once compromised, these devices can be used to launch attacks on other parts of the healthcare network, spreading malware or facilitating data breaches.

Tips to Protect Medical Devices from Cyber Threats

Asset Management and Inventory: Maintain a detailed inventory of all medical devices, including their make, model, software versions, and network connectivity. Automated asset discovery tools can help track devices and monitor their status continuously.

Baseline Network Traffic and Behavior: Establish baseline behaviors for medical devices to detect anomalies. Understanding normal communication patterns helps in identifying suspicious activities that could indicate a cyber attack.

Segmentation and Isolation: Implement network segmentation to isolate medical devices from other critical parts of the healthcare network. This limits the spread of malware and protects sensitive data from unauthorized access. Use virtual local area networks (VLANs) and firewalls to restrict communication to only necessary devices and services.

Regular Software Updates and Patching: Ensure that all medical devices are regularly updated with the latest security patches and firmware updates provided by manufacturers. Vulnerability management practices should include timely patching to mitigate known risks .

Strong Access Controls: Implement robust identity and access management (IAM) practices. Use multi-factor authentication (MFA) for device access and ensure that only authorized personnel can configure or use medical devices .

Encryption and Data Protection: Encrypt data stored on and transmitted by medical devices to protect against unauthorized access. Ensure that devices comply with data protection regulations and standards to safeguard PHI and PII .

Incident Response and Monitoring: Develop a comprehensive incident response plan that includes procedures for addressing cybersecurity incidents involving medical devices. Continuous monitoring and real-time alerts can help detect and respond to threats promptly.

Collaboration with Manufacturers: Work closely with device manufacturers to ensure they provide timely updates and support for cybersecurity measures. Request detailed security information, such as Manufacturer Disclosure Statements for Medical Device Security (MDS2) and Software Bills of Materials (SBOMs) .

Conclusion

The integration of network-connected medical devices in healthcare has revolutionized patient care but also introduced significant cybersecurity challenges. Protecting these devices requires a multi-faceted approach that includes asset management, behavior monitoring, network segmentation, regular updates, strong access controls, encryption, and robust incident response plans. By implementing these practices, healthcare organizations can mitigate the risks posed by cyber threats and ensure the safety and privacy of their patients. For more detailed information on how to protect Network Connected Medical Devices check out HICP Technical Volume 2 HERE!

The Increasing Risks to Cloud Security and Telehealth in Healthcare

The rise of telehealth services has revolutionized the healthcare industry, providing critical access to medical care for underserved communities and enhancing the overall reach of healthcare providers. The ability to conduct remote consultations, monitor patients via connected devices, and manage health records online has been a game-changer, especially in rural and underserved areas. However, while these advancements bring substantial benefits, they also introduce significant risks to cloud security. As healthcare organizations increasingly rely on cloud-based systems to store and manage sensitive patient data, the potential for cyber threats and data breaches has escalated, necessitating robust security measures to safeguard this vital information.

Risks Associated with Cloud and Telehealth

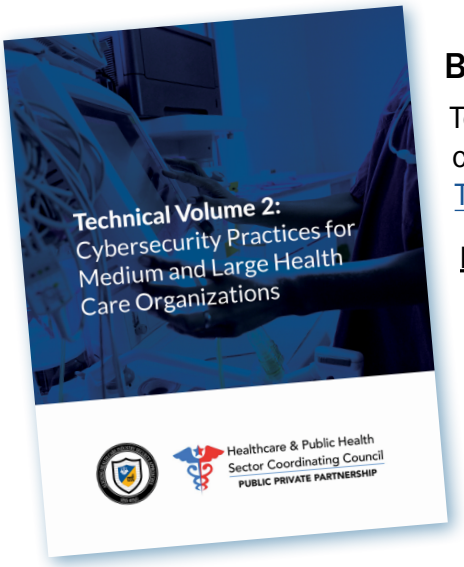
Cloud Computing Risks

The adoption of cloud computing in healthcare brings several benefits, including scalability, cost efficiency, and improved accessibility. However, it also introduces significant cybersecurity risks. One of the primary concerns is the potential for data breaches. Healthcare data is highly valuable on the black market, and cybercriminals target cloud storage systems to access large volumes of patient information.

Telehealth Security Risks

Telehealth services have surged in popularity, especially in the wake of the COVID-19 pandemic. While telehealth provides critical access to care, it also poses several security risks:

- **Unsecured Communication Channels:** Telehealth consultations often use video conferencing tools that may not be secure, leading to potential interception of patient data.
- **Inadequate Device Security:** Both patients and healthcare providers may use personal devices that lack proper security measures.
- **Data Integrity and Authenticity:** Ensuring the data transmitted during telehealth sessions is authentic and untampered is crucial for accurate diagnosis and treatment.



Best Practices for Securing Cloud and Telehealth Systems

To mitigate these risks, healthcare organizations should implement robust cybersecurity practices. The following best practices, drawn from the HICP Technical Volume 2 publication can assist in securing cloud environments:

Implement Strong Access Controls

- **Multi-Factor Authentication (MFA):** Require MFA for all access to cloud-based systems to ensure that only authorized users can access sensitive data.
- **Role-Based Access Control (RBAC):** Limit access to data based on the user's role within the organization, ensuring that individuals only have access to the information necessary for their job.

Encrypt Data

- **Data Encryption:** Encrypt data both in transit and at rest. This ensures that even if data is intercepted or accessed by unauthorized individuals, it remains unreadable without the decryption key.
- **Email Encryption:** Implement email encryption to protect sensitive information shared via email. Regularly monitor and manage encryption practices to detect any anomalies.

Secure Telehealth Communication

- **Use Secure Platforms:** Ensure that telehealth services utilize platforms that comply with industry security standards, such as end-to-end encryption for video calls.
- **Patient and Provider Education:** Train both patients and healthcare providers on the importance of using secure networks and devices for telehealth sessions.

Regular Audits and Monitoring

- **Conduct Regular Security Audits:** Regularly audit cloud and telehealth systems to identify and address vulnerabilities.
- **Implement Continuous Monitoring:** Use advanced monitoring tools to detect suspicious activities and respond promptly to potential security incidents.

Vendor Management

- **Vendor Security Assessments:** Conduct thorough security assessments of third-party vendors who provide cloud and telehealth services to ensure they adhere to security best practices.
- **Contractual Security Requirements:** Include stringent security requirements in contracts with vendors to ensure they are legally obligated to protect your data.

By adopting these best practices laid out in HICP, healthcare organizations can significantly reduce the risks associated with cloud and telehealth services, ensuring the protection of sensitive patient data and maintaining compliance with regulatory standards.

In conclusion, while cloud and telehealth technologies offer significant benefits to healthcare, they also introduce new security challenges. Proactive measures and robust cybersecurity practices are essential to safeguard healthcare data in this continuously evolving digital landscape.

Other Links

Update: Palo Alto Networks Firewalls

Office of Civil Rights

The Biden-Harris Administration Issues New Rule to Support Reproductive Health Care Privacy Under HIPAA

HHS Office for Civil Rights Imposes a Civil Monetary Penalty on New Jersey Nursing Facility for Failing to Provide Timely Access to Patient Records

About The 405(d) Post

This newsletter is for information purposes only and aims to broaden awareness and align healthcare security approaches. The "A Word from the Task Group" and the "405(d) Chronicles" is written by a different 405(d) Task Group Member each issue and does not reflect the views of HHS as a whole. All Task Group Members have been invited to contribute to this newsletter. The news articles are not an endorsement of any product/viewpoint/entity. Use of this document is neither required by nor guarantees compliance with federal, state, or local laws. Please note that the information presented may not be applicable or appropriate for all health care providers and organizations.

Need To Contact Us? Email us at cisa405d@hhs.gov

Follow us!

Facebook X

Instagram LinkedIn

Visit our website at 405d.hhs.gov!