ASPEK HUKUM TELEMEDICINE

HOSIZAH

Prodi D3 Rekam Medis dan Informasi Kesehatan

Universitas Esa Unggul Jakarta

POKOK BAHASAN

1. Langkah-langkah Program Telemedicine
2. Persyaratan *Privacy* dan *Security* Telemedicine

LANGKAH-LANGKAH PROGRAM TELEMEDICINE

- Langkah 1: *Assess and Define*
- Langkah 2: *Develop and Plan*
- Langkah 3: *Implement and Monitor*

LANGKAH 1: *ASSESS AND DEFINE*

1. Identify and document the need and rationale for the envisioned telemedicine program
2. Define the healthcare or other services your telemedicine program will deliver
3. Describe how the targeted services will be delivered
4. Perform a market analysis to determine if there is a market for the service you are proposing to provide and a willingness and mechanism to pay for it
5. Define who “owns” the record
6. Define who is responsible for the amendment, release of information, policies on breach handling, etc.
7. Determine if the telemedicine program scope will cross state lines

LANGKAH 2: *DEVELOP AND PLAN*

1. Use all the information collected in Step 1 to create a plan that details all the areas that require work during the implementation
2. Define all the tasks needed to build, test, deploy, and operate the program
3. Determine who will be needed to perform the tasks
4. Estimate the hours required to do the work (effort)
5. Estimate the timeline for the work
6. Determine if additional staff are required in certain areas
7. Develop a plan to monitor program performance and evaluate the program

LANGKAH: *IMPLEMENT AND MONITOR*

1. Put into action the plans, decisions, and approaches identified in Step 2
2. Begin monitoring the program using the approaches identified in Step 2

PRIVACY AND SECURITY REQUIREMENTS

PERSYARATAN PRIVACY DAN SECURITY

1. Secure Telemedicine Technology and Solutions
2. Internet of Things (IOT)
3. Supplemental Resources

1. SECURE TELEMEDICINE TECHNOLOGY AND SOLUTIONS

1. Secure interfaces between organization and external healthcare agency or business associate **» Encryption of transmitted data and information is required**
2. Secure interfaces between organization and internet providers or application platforms **» Encryption of transmitted data and information is required » Host of internet platform must be determined**
3. Sound Internet of Things (IoT) architecture and visibility across all IoT devices **» Adopt integrated and scalable IoT devices with advanced identification verification mechanisms**
4. Secure mobile health (mHealth) devices

1. SECURE TELEMEDICINE TECHNOLOGY AND SOLUTIONS

5. Ability to integrate telemedicine documentation and records into the patient's existing electronic health record **» New patients should be integrated as would any other new patient record**
6. The telemedicine technology must meet all HIPAA security requirements
7. Non-disruptive security capabilities
8. Ability to provide real-time virtual interactions between patient and provider, between telemedicine hub station and provider, or between an out-of-organization external provider and provider

IG PRIVACY AND SECURITY AND IT GOVERNANCE BEST PRACTICES

1. Use HIPAA-compliant messaging, voice and file transfer, and information storage, which will enable physicians to consult securely with patients
2. Provide effective and compliant storage: Patient information must be stored in secure data centers that regularly conduct risk assessments with policies in place for reviewing controls
3. Integrate with existing communication systems, such as email, SMS, applications and pagers, as well as mobile phones and tablets
4. Securely distribute and access sensitive information from a mobile device, transmit media over industry-standard 256-bit Secure Socket Layer (SSL) encrypted connections, and prevent access by unauthorized users or noncompliant devices
5. Leverage unique user identities, including user names and passwords, and authenticated and rolebased access at both the physical and IT level
6. Provide clear auditing ability for monitoring data integrity and access issues

2. INTERNET OF THINGS (IOT)

- IoT devices are an inherent piece of a telemedicine program.
- These devices must be integrated through sound technology architecture and the visibility of these devices is fundamental in identifying risks and vulnerabilities.
- Organizations should adopt an integrated framework for IoT devices that is not only scalable for future technology additions, but also has identification verification functionalities for optimal and safe care outcomes

3. SUPPLEMENTAL RESOURCES

Telehealth Resource Centers: Privacy, Confidentiality, and Security dapat diakses pada https://www.telehealthresourcecenter.org/toolbox-module/privacy-confidentiality-and-security