LEGALITAS REKAM KESEHATAN ELEKTRONIK (RKE)

Deskripsi: (hlm 71)

Lima isu utama dalam legalitas RKE, yaitu *retention and durability* (retensi dan daya tahan), *storage* (penyimpanan), *signature* (tanda tangan), *accuracy of entries* (keakuratan entri), *transmission integrity (*integritas transmisi). Untuk deskripsi lebih lengkap dapat dibaca pada dalam buku "Electronic Health Records" halaman 71.

1. *retention and durability*

> *Retention and durability* ensures that electronic data follow required retention schedules and can be retrieved from the electronic media on which they are stored. There have been concerns in the past that some electronic media failed to last a long time because they were so new. Optical disks were of particular concern. However, simulations have been performed on optical disks to determine and correct any untoward effects of the aging process. By now, most current electronic media have passed the test of time, but new forms of media may emerge that also must have appropriate testing and **contingency plans** to ensure durability. Contingency plans with respect to media durability often include recopying data onto new media. Reliable evidence of the chain of copying must be preserved.

2. *Storage*

> *Storage* refers to safeguarding data against loss, destruction, tampering, and unauthorized use. These are the same principles that the HIPAA privacy and security rules espouse. Obvious safeguards would include everything from data backup plans, emergency mode operation plans, and disaster recovery plans to workforce and physical security, device and media controls, workstation use and security, access control, audit controls, authentication measures, integrity controls, and transmission controls. Not as obvious but just as important are the administrative security requirements of risk analysis and management, having an information security official, performing clearance checks on members of the workforce, ensuring that incident reporting and response mechanisms are in place, having a means for ongoing monitoring and evaluation, and ensuring that a chain of trust has been established contractually with one's business associates so they adhere to the same standards. Providers should establish **minimum necessary use standards** that are supported by **information access management** processes and technical access controls as well as **audit controls** to provide the ability to examine activity in their information systems. Policies, procedures, and workforce training need to be in place to ensure that uses and disclosures are made only as permitted or required by federal and state law.

3. *Signature*

Signature issues are of major concern for EHRs because many healthcare actions rely on an order being signed, not only by an individual authorized to have access but one credentialed to issue the order. Documentary evidence of action depends on the signature's authenticity. In some respects, EHRs make authentication easier: Entries can be stamped automatically with date, time, and user identification. This provides the elements of an **electronic signature**. Added to that can be **encryption** and **nonrepudiation** (the ability for one not to claim a signature is not his or hers), which would create a **digital signature**. (See figure 3.1 for types of signatures in EHRs.) Whatever form of signature is used, controls must be in place to ensure that the signature elements are not altered or deleted. Additionally, controls must ensure that the individuals using electronic or digital signatures are actually who they claim to be. This is the intent of authentication measures such as passwords, tokens, and biometrics. It also is the intent of nonrepudiation controls in a digital signature. No state or federal laws pertaining to health information requires a digital signature, but some providers are evaluating their use in certain situations.

Figure 3.1. Forms of signatures in the EHR

- **Digitized signature**—Scanned image of a wet signature. This is considered weak because someone could acquire a copy of the image and use it without the person's knowledge.
- **Electronic signature**—Application of a password to an electronic document. This is often used for signing transcribed dictation or orders in a CPOE system. It can be strengthened by using two-tiered authentication (for example, password and token) or biometrics.
- **Digital signature**—Cryptographic signature that authenticates the user, provides nonrepudiation, and ensures message integrity.

Source: Adapted from Cohen and Amatayakul 2003, p. 16.

4. *Accuracy of entries*

Accuracy of entries has always been a concern, whether in paper or electronic forms. Several states require ongoing verification of accuracy, although none have specific technical requirements. In general, documentation accuracy has been a function of quality reviews often performed retrospectively. State and federal laws and regulations have tried not to require specific information technology associated with checking accuracy because of how rapidly technology changes. However, EHR systems are being built with significant edit checking and reminders about proper documentation, which can only enhance compliance with such requirements.

5. *Transmission integrity*

> *Transmission integrity* refers to controls placed on data when they are sent to another entity. HIPAA's Security Rule defines *electronic transmission* as "the exchange of information in electronic media that may occur through the Internet, an extranet that is accessible only to collaborating parties, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media" (45 CFR 160.103[2]). Each means of transmission affords greater or lesser protection of data. The Internet is considered the least protected; physical movement of media is considered the most protected. HIPAA requires transmission controls, including that providers address **integrity** and encryption as they may be needed for the means of transmission involved. The Centers for Medicare and
>
> Medicaid Services (CMS) has a policy that does not permit the transmission of PHI to it through the Internet without encryption.

Hasil pembahasan lima isu utama hukum (legalitas) RKE adalah catatan yang dapat diterima di pengadilan, yang dapat dianggap sebagai bukti terbaik, dan mendukung mosi penemuan, yaitu *Admissibility, Evidence, Discoverability, E-discover,* dan *Metadata.*

1. Admissibility

> *Admissibility*, evidence, and discoverability are important legal concepts that are essentially the result of the five key measures laws and regulations require of any form of health record. **Admissibility** refers to the fact that health records are business records. Because business records are a compilation of many different persons' recordings, they are hearsay. Although there is some variation in how states treat business records, all have some way to except the hearsay rule and allow the records to be used in court. In general, a record custodian must testify that the record was compiled in the normal course of business. This is true in an electronic world as well as a paper or hybrid world.

2. Evidence

> *Evidence* refers to the matter of producing the original or other readable output of a record placed into evidence in court. Microfilm or any other form of miniaturization or electronic storage are deemed equivalent to the original by most courts today. What may dismay some who would produce a paper copy of an EHR for court is that the EHR may not look exactly like the paper copy did in the past, or it may need to be generated from multiple locations. As a result, some hospitals continue to print all documentation from source systems and then scan that material back into an electronically accessible EDMS. Although this is not necessary from a legal perspective, each hospital should evaluate all factors to determine a best practice for its own environment. A completely paperless record all contained in one location can be very convenient. However, many physicians do not like accessing scanned documents and may prefer to access original results from the source systems. Alternatively, they may do neither in the hospital, relying on staff to print out what is needed from whatever source in which it resides or relying on a discharge summary as a means to review previous admission data for a readmission.

3. *Discoverability,*

Discoverability is another important concept. *Discovery* refers to the process in the pretrial phase of a lawsuit where each party can obtain evidence from the opposing party under the law of civil procedure. Such discovery requests include asking for answers to specific questions, production of documents, depositions, and subpoenas. When discovery requests are objected to, a motion can be filed with the court to compel discovery. The court may find it appropriate to grant the request to compel discovery, or it may be swayed that the information sought is not actually relevant, not reasonably accessible, or there was no duty to preserve the information.

4. *E-discover*

E-discovery refers to Amendments to Federal Rules of Civil Procedure and Uniform Rules Relating to Discovery of Electronically Stored Information, which many states are also adopting. E-discovery focuses on the information that surrounds electronic records, often called metadata. This is information typically not included in what generally has constituted the health record in a paper environment,

often referred to as the legal health record. Metadata substantiate the authenticity, accuracy, timeliness, and other elements of an electronic record.

5. *Metadata.*

Metadata in or associated with an EHR include date/time stamps, audit logs, clinical practice guidelines, evidence of the provision of clinical decision support, access to knowledge databases, information system activity review logs, and other information. There is still controversy surrounding just exactly where the "record" ends and other functionality begins. AHIMA's concept of the legal health record may serve as guide for preparing the record for court. It is a good idea for each organization to have its own policy and procedure to support this process, which is likely to change several times along the migration path to the EHR (Servais 2008; McLendon and Lowe 2011). Care should be taken to follow the organization's legal health record and/or retention policies closely, as any variance could be viewed as spoliation of evidence. The spoliation of evidence doctrine relates to the act of holding from destruction those records that are the subject of pending or potential litigation or investigation. Destroying such a record (spoliation) could be viewed by the courts as the equivalent of obstruction of justice in a criminal case. Courts may impose sanctions for destroying records relevant to pending or even potential litigation. These may include not allowing documents introduced at trial, special jury instructions, financial sanctions, fines, imprisonment, or even a new lawsuit in certain states.