


LEGAL REQUIREMENT FOR TELEMEDICINE

HOSIZAH

Prodi D3 Rekam Medis dan Informasi Kesehatan

Universitas Esa Unggul Jakarta



LEGAL REQUIREMENTS

1. Preventing Telemedicine Fraud And Abuse: An Information Governance Approach
2. Compliant Business Associate Agreements (BAA)
3. Cross-state Licensure
4. Anti-trust Laws
5. Federal Anti-kickback Statute
6. Supplemental Resources

1. PREVENTING TELEMEDICINE FRAUD AND ABUSE: AN INFORMATION GOVERNANCE APPROACH

- New systems, new technologies, new processes, and new staff resources are opportunities for fraud and abuse. These new weaknesses often have not all been identified or addressed leaving systems and technologies vulnerable.
- A new or existing telemedicine program should work to proactively address all vulnerabilities and manage risks.
- To address and prevent fraud and abuse proactively in the telemedicine healthcare delivery setting, it is beneficial to have an IG program team approach. The IG team, which includes legal representatives, can provide legal counsel and incorporation of the telemedicine program into the organizations overall fraud and abuse compliance programs.
- Important issues such as state self-referral, kickback laws, corporate practice of medicine, licensing, joint ventures, contractual arrangements, and liability risk management are all issues that could help be addressed by strong IG leadership, the appropriate IG stakeholders, and effective collaboration

2. COMPLIANT BUSINESS ASSOCIATE AGREEMENTS (BAA)

- The CE should set an expectation in the BAA that the BA maintains security that adheres to all requirements. If a potential breach occurs, the CE should lead an investigation with the assistance of the BA.
- According to AHIMA's "Guidelines for a Compliant Business Associate Agreement," "The plan of action should include: an audit plan, four-step risk assessment, response triggers, communication protocol, chain of command, contact information, education, training, mitigation process, breach notification timeliness, content, methods of the notice, and back-up contact information for key responsible parties at the BA and CE."

2. COMPLIANT BUSINESS ASSOCIATE AGREEMENTS (BAA)

- Compliance with HIPAA and the HITECH (Health Information Technology for Economic and Clinical Health) Act are top priorities for all healthcare delivery organizations and their business associates. Telemedicine is centered on technology functions and is transmitted through a variety of platforms.
- It is critical that HIPAA and HITECH compliance is met in all aspects of telemedicine to ensure the most effective patient outcomes as well as the privacy and security of patient information. Healthcare organizations must obtain business associate agreements from a number of associated parties including but not limited to: Compliance with HIPAA and the HITECH (Health Information Technology for Economic and Clinical Health) Act are top priorities for all healthcare delivery organizations and their business associates. Telemedicine is centered on technology functions and is transmitted through a variety of platforms.
- It is critical that HIPAA and HITECH compliance is met in all aspects of telemedicine to ensure the most effective patient outcomes as well as the privacy and security of patient information. Healthcare organizations must obtain business associate agreements from a number of associated parties including but not limited to:
 - Telemedicine hardware vendors (domestic and offshore)
 - Telemedicine software vendors (domestic and offshore)
 - Medical device vendors
 - Non-HIPAA covered entities
 - Providers/Clinics where patients may utilize their internet services for telemedicine

2. COMPLIANT BUSINESS ASSOCIATE AGREEMENTS (BAA)

- Notice of Privacy Practices Telemedicine practices must follow the same HIPAA regulations for the notice of privacy practices (NPP).
- Providers must inform the patient or the patient's legal representative of how their protected health information can be used or accessed.
- Information is more readily available to healthcare providers and it is necessary to address this in the NPP.
- This must be adequately documented in the patient's record. For more information, refer to the HHS Notice of Privacy Practices for Protected Health Information rule

3. CROSS-STATE LICENSURE

Cross-state licensure is a challenge that is being addressed as telemedicine practices expand. For a provider to practice, they must attain licensure in the state where the patient is located. With telemedicine, the originating site of the patient is considered the place of service, and therefore the provider must adhere to the licensing rules of the state in which the patient is located. Similar guidelines are followed when looking at malpractice lawsuits regarding cross-state practicing, where no coverage is provided when a provider is not licensed in a particular state.

The Telehealth Resource Centers provide information about cross-state licensure .

4. ANTI-TRUST LAWS

Anti-trust laws stop anticompetitive behavior and ensure fair pricing. They exist to promote competition among companies, which results in lower prices, more choices for consumers, and better products for a consumer to choose from. Anti-trust can arise in the telemedicine market. According to the Telehealth Resource Centers:

- “Antitrust concerns may arise in certain situations involving telehealth. Electronic health records would most likely include not only clinical information, but also payment information, creating the potential for price collusion. Where one provider has access to the pricing policies of another provider (other than through open advertising) “price fixing” can occur. Price fixing is an anti-trust violation and can lead to penalties. This may create a barrier to the development and use of systems unless proper safeguards are put in place. Telehealth networks that provide equipment to remote underserved community sites at less than fair-market value to promote the development of services and referral patterns in underserved communities may risk being challenged for violating anti-trust as well as Stark laws if such actions create a monopoly”.

Additional resources on anti-trust laws are available from the Federal Trade Commission and the US Department of Justice.

5. FEDERAL ANTI-KICKBACK STATUTE

- The federal anti-kickback statute is designed to protect healthcare programs and clients from fraud and abuse, specifically regarding monetary fraud and abuse.
- This statute can be violated anytime a person receives monetary benefit in return for receiving CMS funds (typically through referring patients).
- Much technology is available today to encourage and make referrals easier, and if a particular referral results in being reimbursed by the federal government, it is a violation of the federal anti-kickback statute. More examples and exceptions (called “safe harbors”) to the kickback statutes can be found under 42 CFR 1001.952 and 42 U.S. Code § 1320a–7b.

6. SUPPLEMENTAL RESOURCES

- Resources pertaining to other legal guidelines include the Stark Law, Federal Communication Commission and Telehealth, and the Food and Drug Administration:
- Stark Law <http://www.telehealthresourcecenter.org/toolbox-module/federal-fraud-and-abuse-stark-law> <https://www.law.cornell.edu/uscode/text/42/1395nn> C & Telehealth <http://www2.itif.org/2012-mhealth-taskforce-recommendations.pdf> <http://www.telehealthresourcecenter.org/toolbox-module/federal-communications-commission-and-telehealth>
- FDA <http://www.telehealthresourcecenter.org/toolbox-module/food-and-drug-administration-and-state-regulations> <https://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/default.htm>