OPTUM™

Telemental Health

Choosing a Telehealth Vendor

In order to qualify for reimbursement, technology used to deliver telehealth services must be compliant with applicable federal regulations including HIPAA (Health Insurance Portability and Accountability Act) and HITECH (Health Information Technology for Economic and Clinical Health Act). HIPAA includes both a Privacy Rule and a Security Rule designed to protect the Personal Health Information (PHI) of patients while providing appropriate access to PHI by providers and other healthcare entities. HITECH expands the scope of HIPAA privacy and security protections, increases the potential liability for non-compliance, and provides for more strict enforcement of HIPAA provisions.

HIPAA applies to 'covered entities' which include: healthcare providers, health plans and healthcare clearing houses. HIPAA also applies to 'Business Associates' of covered entities. If a covered entity engages a business associate to help carry out its health care activities and functions, the covered entity and associate must execute a written Business Associate Agreement that establishes what the Business Associate has been engaged to do, and requires the Business Associate to protect the privacy and security of protected health information.

HIPAA has specific regulations for electronic delivery of PHI. HIPAA would therefore govern telehealth delivery services. Therefore, covered entities must ensure that the technology utilized to deliver telehealth services is compliant with the provisions of HIPAA/HITECH, and that Business Associate Agreements are in place where required.

There are hundreds of telehealth-related products available on the market, and multiple technologies are often utilized in combination during the delivery of telehealth services. Therefore, maintenance of an up-to-date comprehensive list of compliant technologies is not feasible. Following are helpful guidelines that may be useful when evaluating whether a particular telehealth technology solution is compliant with the provisions of HIPAA and HITECH regulations.

Does the vendor claim HIPAA compliance?

Due to industry recognition of the critical nature of HIPAA compliance in this area, vendor statements regarding compliance are usually prominently posted on their website and other product materials. While a vendor's claim of HIPAA/HITECH compliance is not necessarily a guarantee and does not alleviate a covered entity's due diligence, it is a good initial indicator of compliance and should be on your list of requirements when evaluating prospective vendors.

Will the vendor sign a Business Associate Agreement (BAA)?

Telehealth service delivery includes a number of scenarios where the technology electronically stores or transmits personally identifiable information/ personal health information (PII/PHI) data between parties, such as during a videoconference, a text chat, appointment scheduling, screen sharing, file sharing and conference recording. Therefore, in most cases, unless an exception is available, the covered entity must execute a Business Associate Agreement with the vendor that provides the telehealth enabling technology. Again, willingness to sign a Business Associate Agreement should be on your list of requirements when evaluating prospective vendors.

The 'Conduit Exception':
If the technology serves strictly as a simple conduit for data, then it may fall under the conduit exception as described within the HIPAA Final Rule. In order to meet the definition of "conduit", the vendor must not have access to the telehealth session encryption key or data stream, and must not store PII/PHI data. In that case, a BAA may not be required. Each covered entity must conduct its own due diligence to assure its compliance.

Will the vendor provide validated results of vulnerability scans of their system?

Vendors should supply prospective customers with the results of vulnerability scans of their products. Ideally, vulnerability scans are conducted by third parties who supply detailed documentation regarding results of the scan. Vulnerability scans should be conducted on a regular basis. Minimally, the vendor should supply their own documented vulnerability scan results using an industry standard scanning technology. If the vendor will not, or is not able to provide you with vulnerability scan results, you should consider this in your due diligence analysis.

Does the vendor solution utilize encryption to protect data, both at rest and in transit?

Data encryption technology should be used to secure and keep private PII/PHI data that is either at rest (stored on a hard drive for example) or in transit (as in during a videoconference). In the case of videoconferencing, the risk is that an unencrypted video or audio data stream could be intercepted by unauthorized parties providing them with access to protected information under the HIPAA privacy rule. Therefore, an industry-standard encryption scheme should be applied to all data streams that pass between sites through the telehealth system. Ideally, the media stream should be encrypted end-to-end (from one telehealth site to the other) and the technology vendor does not have access to the data encryption key which could be used to intercept and decode the data stream. This is not always the case, for example, if the product architecture provides the system administrator with access to both the encryption key and the data stream for monitoring purposes, then this may not meet the conduit exception.

Equally important, persistent PII/PHI data that is stored at any location (local computer, cloud storage, network drive etc.) should also be encrypted in order to prevent

unauthorized access or a breach. In the event that unauthorized access does occur, events involving unencrypted data will increase your potential liability and exposure to penalties. So, be sure to verify with your prospective vendors:

- Whether any PII/PHI data is stored on their system
- If so, that any stored PHI/PII is encrypted using appropriate industry standard technology.

The Covered Entity's role in maintaining HIPAA compliance when delivering telehealth services:

In addition to the enabling technology, the policies, procedures and protocols used in delivering telehealth services must also be evaluated for HIPAA/HITECH compliance.

Examples of telehealth operational areas that should be carefully examined include:

- Procedures/protocols to ensure that unauthorized third parties cannot join, record or listen in on a videoconference
- Procedures/protocols to ensure that if video or audio conferences are recorded, the recordings are securely stored (preferably as encrypted files), have strict access controls in place, and are correctly identified
- Procedures/protocols for initiating inbound or outbound videoconference calls
- Protocols are in place for use of text chat, screen-sharing, and file-transfer features
- Procedures/protocols to ensure that telehealth sessions are always conducted in locations that offer adequate patient privacy