The *Statewide Health Information Policy Manual* (SHIPM) developed by the Center for Data Insights and Innovation (CDII) provides an analysis of applicable Federal (including HIPAA) and State laws and regulations related to Telehealth - see SHIPM Chapter 2 – *2.9.1 Requirements for Telehealth* for specific information.

The following checklist is provided to assist your department ensure privacy and security considerations are assessed when implementing your telehealth solution. CDII recommends you print and retain the completed checklist.

| **#** | **Privacy/Security Item** | **Covered (Y or N)** |
| --- | --- | --- |
|  | Use of authorized telehealth equipment - does the equipment have sufficient security features to meet Health Insurance Portability and Accountability Act (HIPAA) and state security requirements? |  |
|  | Are you using a vendor for all or part of the solution? |  |
|  | If yes:   1. What is the vendor providing – equipment, software, connectivity, or a third-party software license with limited support and maintenance? |  |
|  | 1. Does the vendor agreement contain representations and warranties that the equipment will function as warranted, and are there guaranteed uptimes and limited downtimes? |  |
|  | 1. Is the vendor a business associate?  * Does the agreement outline the vendor’s responsibilities in the event of a breach of protected health information (PHI)? * Does the agreement contain indemnification or limitation of liability provisions in the event of a breach? * Does the vendor have cyber liability insurance and other insurance coverage, and are the amounts adequate? |  |
|  | Conduct a security risk analysis of the telehealth equipment to identify any security vulnerabilities and implementing a risk management plan to mitigate vulnerabilities. Each of the originating-site and distant-site parties should conduct its own security risk analysis. |  |
|  | Integration and interoperability of electronic data generated from telehealth services into the electronic health record and health information exchanges. How will the originating site and distant site use and disclose electronic PHI (ePHI)? |  |
|  | Identify authorized users of the telehealth system and electronic health record and ensure access controls are in place to restrict access to only authorized users. |  |
|  | Patient privacy and security during live videoconference between the patient and the distant provider. |  |
|  | Secure transmission of the videoconference between the patient and the distant provider. |  |
|  | Monitor/audit access, use and disclosure of PHI with telehealth services, and responsibilities between the parties. |  |
|  | Revise privacy and security policies and procedures to include the use of telehealth. |  |
|  | Revise the Notice of Privacy Practices to include the use of telehealth for treatment, payment and operations purposes. |  |
|  | Document responsibilities between the parties in the event of a breach of unsecure PHI and notification requirements. |  |
|  | Assess additional federal and state privacy laws applicable to your organization. In addition, consider the protection of sensitive information such as substance abuse, mental health, HIV/AIDS status and other (see SHIPM Chapter 2 – *2.3.0 Specially Protected Information*). |  |
|  | Assess the Federal Trade Commission’s and the Food and Drug Administration’s regulations governing the use of mobile medical apps if mobile apps are being used to communicate with the patient. |  |
|  | Record retention laws for electronic recordings, secure storage, maintenance and transmission of ePHI, and responsibilities of the parties. |  |