



THIRD PARTY SERVICE PROVIDER QUESTIONNAIRE

Entity:	
Name & Title of Organization Senior Officer:	
Name of Organization Cybersecurity/Technology Contact:	
Email:	Phone:
Do you encrypt nonpublic information both in transit and at rest?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Do you employ access controls designed to limit access to relevant information systems and nonpublic information?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Do your access controls include additional measures to prevent access to your internal networks from an external network, such as the use of Multi-Factor Authentication or Risk-Based Authentication? Please check NA if you do not allow remote access to your internal networks.	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> NA
Do you have policies and procedures in place to notify our organization in the event of a cybersecurity event that directly impacts our information systems or nonpublic information?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Click here to attest that the above is true and accurate to the best of your knowledge.	<input type="checkbox"/>
Name & Title of person completing form:	
Date:	

- Definition of NPI:** Nonpublic Information shall mean all electronic information that is not Publicly Available Information and is: (1) Business-related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity; (2) Any information concerning an individual, which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) driver's license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records; (3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.
- Definition of cybersecurity event:** Any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.