

Central Islip Union Free School District Program Information and Data Privacy Third Party Agreement



To be completed **by the vendor** and submitted for all NEW and RENEWAL software/programs prior to purchase/implementation. Refusal of the vendor complete this agreement may serve as cause for the district to see similar services through another program and/or vendor.

Software/Program Title:	ImPACT Test for assessment and management of concussion
Publisher:	ImPACT Applications, Inc.
Contract Pricing	<input type="checkbox"/> BOCES Contract or Shared Service <input type="checkbox"/> NYS or Federal Contract Pricing <input checked="" type="checkbox"/> Direct Pricing, Bid or RFP with Vendor <input type="checkbox"/> Free Version/Freemium
Single-Sign-On Options	<input type="checkbox"/> SSO Available through Azure AD/SAML <input type="checkbox"/> SSO through Clever <input type="checkbox"/> NO SSO Option <input checked="" type="checkbox"/> N/A - Non-User Based Program/Not Applicable
License Structure:	<input type="checkbox"/> Per-User <input type="checkbox"/> Per-Student <input type="checkbox"/> Per-Teacher/Classroom <input checked="" type="checkbox"/> Per-Building <input type="checkbox"/> Districtwide/Unlimited <input type="checkbox"/> N/A - Not Applicable or Free Version
SIS-PowerSchool Integrations	<input type="checkbox"/> Program DOES NOT sync to SIS (PowerSchool) <input type="checkbox"/> Program DOES sync to SIS (PowerSchool) <input checked="" type="checkbox"/> N/A - Not Applicable

ALL LINKS MUST BE PROVIDED AND COMPLETED BY THE VENDOR!

Software Title:	ImPACT Test for assessment and management of concussion
Publisher/Developer:	ImPACT Applications, Inc.
Developer/Vendor Name:	ImPACT Applications, Inc.
Developer/Vendor Mailing Address:	2140 Norcor Avenue, Suite115, Coralville, IA 52241-9736
Developer/Vendor Privacy Policy Link:	https://impacttest.com/privacy-notice/

This Data Privacy Agreement ("DPA") is by and between the Central Islip Union Free School District (herein known as "EA"), an Educational Agency, and the above listed software, app or extension developer (herein known as "Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

- Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor’s security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
- Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
- Disclose:** To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written, or electronic, whether intended or unintended.
- Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
- Educational Agency:** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
- Eligible Student:** A student who is eighteen years of age or older.

7. **Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
8. **NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
9. **Parent:** A parent, legal guardian or person in parental relation to the student.
10. **Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, and Teacher or Principal APPR Data, as defined below.
11. **Release:** Shall have the same meaning as Disclose.
12. **School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
13. **Student:** Any person attending or seeking to enroll in an Educational Agency.
14. **Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
15. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
16. **Teacher or Principal APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. **Compliance with Law:** In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules, and regulations.
2. **Authorized Use:** Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

- 3. Data Security and Privacy Plan:** Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.
- 4. EA's Data Security and Privacy Policy:** State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.
- 5. Right of Review and Audit:** Upon request by the EA, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.
- 6. Contractor's Employees and Subcontractors.**

 - (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.
 - (b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.
 - (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.
 - (d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.
 - (e) Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

- 7. Training:** Contactor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.
- 8. Termination:** The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.
- 9. Data Return and Destruction of Data.**
 - (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the EA, subject to Contractor's medical data retention policies, as outlined in the Contractor's Privacy Notice (available here: <https://impacttest.com/privacy-notice/>) unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required under applicable law, regulation, court order, subpoena, or similar legal process. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.
 - (b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed, subject to Contractor's internal backup data retention policies. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.
 - (c) Upon EA' written request Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.
 - (d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party; provided, Contractor may transfer de-identified data to third parties subject to appropriate confidentiality agreements for the purposes of (i) assessing the quality of and improving the Services and (ii) research and development.
- 10. Commercial or Marketing Use Prohibition:** Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

- 11. Encryption:** Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.
- 12. Breach.**
- (a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.
 - (b) Notifications required under this paragraph must be provided to the EA at the following address: Philip K. Voigt, Director of Technology at Central Islip SD, 50 Wheeler Rd, Central Islip, NY 11722.
- 13. Cooperation with Investigations:** Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.
- 14. Notification to Individuals:** Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.
- 15. Termination:** The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

- 1. Parent and Eligible Student Access:** Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. **Bill of Rights for Data Privacy and Security:** As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. **Priority of Agreements and Precedence:** In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. **Execution:** This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

As the duly authorized officer of the “contractor” as listed above I attest to all of the above submitted information to be true and accept any liability and/or responsibility for any data breeches or intrusions associated with this program, applications, software or browser extension.

DocuSigned by:
Tyler Morrison
A5CDEDB3C063486...

August 22, 2024

Signature of Vendor Official Representative

Date

Tyler Morrison, General Manager, Clinical

If the program does not collect or transmit any PII, this document must still be completed, initialed (pages) and signed but you may and the select “NO PII OR DATA IS COLLECTED OR VIEWABLE” option above. No program/app/extension will be considered without a complete agreement.

EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security


Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to Philip K. Voigt, Director of Technology at Central Islip SD, 50 Wheeler Rd, Central Islip, NY 11722. (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner’s Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Description of the purpose(s) for which Contractor will receive/access PII	<p>Description:</p> <p>ImPACT, an FDA cleared medical device, is used by healthcare, educational, and sports organizations to help assess and manage concussions with the computerized battery of an on-line cognitive tests. ImPACT measures visual and verbal memory, reaction time, and processing speed to help determine if a student (ages 12 and up) can safely return to activity.</p> <p><input type="checkbox"/> NO PII OR DATA IS COLLECTED OR VIEWABLE THROUGH THIS PROGRAM/APP <input checked="" type="checkbox"/> NOT APPLICABLE - NO PII OR DATA IS COLLECTED/VIEWABLE</p>
Type of PII that Contractor will receive/access	<p>Check all that apply:</p> <p><input checked="" type="checkbox"/> Student PII <input type="checkbox"/> Employee PII <input type="checkbox"/> NOT APPLICABLE - NO PII OR DATA IS COLLECTED/VIEWABLE</p>
Contract Term	<p>Each Data Privacy Agreement is valid through the software renewal period or 1 Year for non-paid/free/pilot programs.</p>
Data Transition and Secure Destruction	<p>Upon expiration or termination of the Contract, Contractor shall:</p> <p><input type="checkbox"/> Securely transfer data to EA, or a successor contractor at the EA’s option and written discretion, in a format agreed to by the parties. <input checked="" type="checkbox"/> Upon EA’s written request securely delete and destroy data, subject to Contractor’s internal backup data retention policies and except as required under applicable law, regulation, court order, subpoena, or similar legal process. <input type="checkbox"/> NOT APPLICABLE - NO PII OR DATA IS COLLECTED/VIEWABLE</p>
Challenges to Data Accuracy	<p>Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA’s written/emailed request.</p>
Encryption	<p><input checked="" type="checkbox"/> Data will be encrypted while in motion and at rest. <input type="checkbox"/> NOT APPLICABLE - NO PII OR DATA IS COLLECTED/VIEWABLE</p>

As the duly authorized officer of the “contractor” as listed above I attest to all of the above submitted information to be true and accept any liability and/or responsibility for any data breaches or intrusions associated with this program, applications, software, or browser extension.

DocuSigned by:

A5CDEDB3C063486...

Signature of Vendor Official Representative
Tyler Morrison, General Manager, Clinical

August 22, 2024

Date

ATTACHMENT 1 - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	ImPACT Applications has implemented many policies and procedures as it relates to the security, privacy and availability of our application environments. We undergo annual SOC 2 Type II audits by an independent third-party auditor covering the domains of security, privacy and availability. ImPACT Applications has also achieved ISO 13485 certification for our quality management system. We've also ensured HIPAA Privacy and Security rule compliance.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Administrative, physical and technical safeguards, in congruence with HIPAA's privacy and security rules are part of our company's quality management system and are ingrained in the normal business operations practices. Risk analysis, access control and authorization, physical facility access policies, data backup and encryption all are part of policies that are in place.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	Employees receive training on data privacy and security, HIPAA compliance, various cybersecurity topics and many other internal training courses that are relevant to the employee's job position. These training courses are assigned by the Director of Regulatory Affairs and are tracked through an online system to ensure employee compliance.

4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	Employees are required to read and acknowledge our employee handbook, as well as several other employment related documents upon the start of their employment with the company. Employment doesn't start until all of these agreements are signed.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	Any data security and privacy incidents will undergo discovery and risk assessment, identification of the cause and extent of the breach, foreseeable harm of the breach, and notification of affected customers. Notification to affected customers will occur within 48 hours of becoming aware of the breach.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Customers are able to export their data at any time via the ImpACT Applications Customer Center.
7	Describe your secure destruction practices and how certification will be provided to the EA.	<p>When a machine or hard drive is decommissioned and has been used by an employee with access to Personal Information, the drive must be securely erased or destroyed before the machine, or its hard drive can be relinquished from the company's control. DBAN is our utility of choice, a disk image for a bootable CD can be found at https://dban.org.</p> <p>If the drive has failed, and will not complete a DBAN destruction attempt, the drive must be physically destroyed so the platters inside are crushed, and it is not usable any longer. Document template QT-18 is to be used to create a record of the data destruction, signed, and stored as evidence of the completed action.</p> <p>Data deleted from our production databases as part of our data deletion processes is identified and removed based on the age of the records, and the data retention settings of the</p>

		customer organization. Data is removed by an automated process, executing sql statements to remove the specified information from our online databases. The number of records before and after a data deletion event can be provided to confirm the removal of data.
8	Outline how your data security and privacy program/practices align with the EA’s applicable policies.	Our data security practices were designed to meet and exceed the requirements set by HIPAA and many other state/local entities. Our policies and procedures have been audited as part of our ISO 13485 certification and SOC 2 Type 2 annual audits.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

ATTACHMENT 1(a) – NIST CSF TABLE

The table below will aid the review of a Contractor’s Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework>. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy.	Our systems are housed in a secure datacenter facility, within a locked cabinet. Only authorized employees have access to the computing environment. Access to environments (physical or logical) must be approved by management and allocated to each individual user. Hardware assets are tracked by serial number. The company follows a joiners & leavers process to ensure accounts are provisioned and deprovisioned in a timely fashion. We employ VPNs and MFA to provide secure access for our employees.
	Business Environment (ID.BE): The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this	Our employee handbook defines expected employee behavior. Job descriptions outline roles and responsibilities. Our quality management system helps to assess and manage risk, ensuring our products are secure and compliant from design to delivery.

Function	Category	Contractor Response
	<p>information is used to inform cybersecurity roles, responsibilities, and risk management decisions.</p>	<p>Our ISO 13485 certification and annual SOC 2 Type 2 audits are instrumental in helping to ensure these policies are followed.</p>
	<p>Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.</p>	<p>Our ISO 13485 quality management system has policies and procedures for managing and monitoring the organization’s regulatory, legal, risk, and operational requirements. The policy is distributed to applicable employees, and those that have participatory roles are trained on their responsibilities regarding these policies.</p>
	<p>Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.</p>	<p>ImPACT Applications has controls, procedures and policies in place to reduce and mitigate as much as possible any cybersecurity risk to organizational operations, data, assets, and individuals, including but not limited to secure development practices, network and internet boundary protections, and server protections.</p>
	<p>Risk Management Strategy (ID.RM): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.</p>	<p>ImPACT Applications has a comprehensive risk management strategy that is part of our overall quality management system.</p>
	<p>Supply Chain Risk Management (ID.SC): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.</p>	<p>ImPACT Applications has implemented a vendor evaluation and purchasing process to vet vendors and their products prior to purchase, ensuring they meet the designated criteria for their function.</p>
<p>PROTECT (PR)</p>	<p>Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.</p>	<p>ImPACT Applications follows a Joiners and Leavers process that requires approval for account creation and prompt termination of access that is no longer necessary. This process is audited as part of our annual SOC 2 Type 2 audit.</p>
	<p>Awareness and Training (PR.AT): The organization’s personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.</p>	<p>ImPACT Applications has an employee training program in place and routinely assigns training exercises to employees on an as-needed basis. All employees receive a base-level of training when their employment begins, and additional items are added depending on job function and industry changes.</p>
	<p>Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.</p>	<p>ImPACT Applications ensures all sensitive PII and PHI data are handled appropriately, stored in secure locations, and encrypted in transit and while at rest in our application database.</p>

Function	Category	Contractor Response
DETECT (DE)	<p>Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.</p>	<p>ImPACT Applications has a comprehensive set of IT policies and procedures, reviewed and approved by management that are followed and audited as part of our annual SOC 2 Type 2 audit.</p>
	<p>Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.</p>	<p>ImPACT Applications' IT policies and procedures contain sections addressing maintenance and patching of our systems.</p>
	<p>Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.</p>	<p>ImPACT Applications periodically reviews all firewall rules associated with our application environments to ensure they are appropriate for our application needs. Any changes to the firewall rule set need to be reviewed and approved by management prior to being implemented.</p>
DETECT (DE)	<p>Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.</p>	<p>All servers run HIDS software to monitor for any intrusion attempts and are configured to notify ImPACT Applications system administrators immediately if any anomalies are detected.</p>
	<p>Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.</p>	<p>ImPACT Applications monitors all servers with standard server & resource monitoring software to ensure they are operating properly. Additionally, we perform quarterly vulnerability scans and annual application security scans to check for and resolve any vulnerabilities found.</p>
	<p>Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.</p>	<p>HIDS and WAF configurations are reviewed periodically to ensure proper configuration and notification is in place.</p>
RESPOND (RS)	<p>Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.</p>	<p>ImPACT Applications has a series of policies and procedures in place in the event a security event occurs. This policy includes information about notification requirements and time periods, investigation, and remediation.</p>
	<p>Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).</p>	<p>ImPACT Applications has a defined breach notification procedure that defines the tasks to complete, who to involve, when notifications are to go out and what they should contain.</p>
	<p>Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.</p>	<p>ImPACT Applications procedures include analysis phases to ensure an incident is sufficiently investigated to ensure the root problem is identified and corrected.</p>
	<p>Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.</p>	<p>ImPACT Applications will work to contain and limit the impact of any security event as quickly as possible, while preserving any information that would be helpful in investigating the root cause of the incident.</p>
	<p>Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from</p>	<p>ImPACT Applications will take appropriate actions to mitigate or correct any issues that resulted in the origination of the incident to prevent any reoccurrence in the future.</p>

Function	Category	Contractor Response
	current and previous detection/response activities.	
RECOVER (RC)	<p>Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.</p>	<p>ImPACT Applications has a disaster recovery policy in place, tests the procedure annually, and ensures any required changes to the policy are made as needed.</p>
	<p>Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.</p>	<p>As part of our disaster recovery testing process, any lessons learned are incorporated into the policy so that it is continuously improved and accurate for current systems/applications.</p>
	<p>Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).</p>	<p>ImPACT Applications has direct lines of communication with critical service providers, monitors communications and status pages for providers, alert messages and notifications from critical vendors. We subscribe to notification lists for services, software vendors and other service providers so that we can be aware of any service interruptions that may affect our services and customers.</p>