SandBox Union Written Information Security Program (“WISP”)

The objectives of this comprehensive written information security program ("WISP") include defining, documenting, and supporting the implementation and maintenance of the administrative, technical, and physical safeguards SandBox Union has selected to protect the personal information it collects, creates, uses, and maintains.

1. **PURPOSE**. The purpose of this WISP is to:
    a. Ensure the security, confidentiality, integrity, and availability of personal and other sensitive information SandBox Union collects, creates, uses, and maintains;
    b. Protect against any anticipated threats or hazards to the security, confidentiality, integrity, or availability of such information;
    c. Protect against unauthorized access to or use of SandBox Union-maintained personal and other sensitive information that could result in substantial harm or inconvenience to any customer or employee; and
    d. Define an information security program that is appropriate to SandBox Union's size, scope, and business; its available resources; maintain compliance requirements; and the amount of personal and other sensitive information that SandBox Union owns or maintains on behalf of others while recognizing the need to protect both customer and employee information.

2. **SCOPE**. This WISP applies to all employees, third-party agents, officers, and directors of SandBox Union. It applies to any records that contain personal and other sensitive information in any format and on any media, whether in electronic or paper form.
    a. For purposes of this WISP, personal information shall include:
        i. Personal identifiable or other confidential information (“PII or confidential”), which includes:

            1. Names;
            2. All geographical identifiers smaller than a state, except for the initial three digits of a zip code, if, according to the current publicly available data from the Bureau of the Census: the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000;
            3. Dates (other than year) directly related to an individual;
            4. Phone numbers;

5. Fax numbers;
6. Email addresses;
7. Social Security numbers;
8. Medical record numbers;
9. Health insurance beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Uniform Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger, retinal, and voice prints;
17. Full-face photographic images and any comparable images; or
18. Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data.

b. Personal information does not include:
   i. lawfully obtained information that is available to the general public, including publicly available information from federal, state, or local government records;
   ii. any data that could not be used to identify a patient; or
   iii. internal identifiers that SandBox Union could use to identify a patient, but any external parties would not be able to use them to identify a patient.

c. For purposes of this WISP, “sensitive information” means data that (i) SandBox Union considers to be highly confidential information; or (ii) if accessed by or disclosed to unauthorized parties, could cause significant or material harm to SandBox Union, its customers, or its business partners. Sensitive information includes but is not limited to, personal information.

3. **INFORMATION SECURITY COMPLIANCE TEAM.** SandBox Union has designated the Director of Infrastructure and Information Security and the General Counsel to implement, coordinate, and maintain this WISP (the "Information Security Compliance Team"). The Information Security Compliance Team shall be responsible for the following:
   a. Initial implementation of this WISP, including:

i. Assessing internal and external risks to personal and other sensitive information and maintaining related documentation, including risk assessment reports and remediation plans (see Section 4);
ii. Coordinating the development, distribution, and maintenance of information security policies and procedures (see Section 5);
iii. Coordinating the design of reasonable and appropriate administrative, technical, and physical safeguards to protect personal and other sensitive information (see Section 6);
iv. Ensuring that the safeguards are implemented and maintained to protect personal and other sensitive information throughout SandBox Union, where applicable (see Section 6);
v. Overseeing service providers that access or maintain personal and other sensitive information on behalf of SandBox Union (see Section 7);
vi. Monitoring and testing the information security program's implementation and effectiveness on an ongoing basis (see Section 8);
vii. Defining and managing incident response procedures (see Section 9); and
viii. Establishing and managing enforcement policies and procedures for this WISP, in collaboration with SandBox Union human resources and management (see Section 10).

b. Employee, contractor, and stakeholder training, including:
i. Providing periodic training regarding this WISP, SandBox Union's safeguards, and relevant information security policies and procedures for all employees, contractors, and stakeholders who have or may have access to personal or other sensitive information;
ii. Ensuring that training attendees formally acknowledge their receipt and understanding of the training and related documentation through written acknowledgment forms; and
iii. Retaining training and acknowledgment records.

c. Reviewing the WISP and the security measures defined herein annually or whenever there is a material change in SandBox Union's business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal or other sensitive information (see Section 11), following a Plan, Do, Check, Act (“PDCA”) cycle.

d. Defining and managing an exceptions process to review, approve or deny, document, monitor, and periodically reassess any necessary and appropriate, business-driven requests for deviations from this WISP or SandBox Union's information security policies and procedures.

e. Periodically reporting to SandBox Union management regarding the status of the information security program and SandBox Union's safeguards to protect personal and other sensitive information.

4. **RISK ASSESSMENT.** As a part of developing and implementing this WISP, SandBox Union will conduct a periodic, documented risk assessment annually or whenever there is a material change in SandBox Union's business practices that may implicate the security, confidentiality, integrity, or availability of records containing personal or other sensitive information.

a. The risk assessment shall:
    i. Identify reasonably foreseeable internal and external risks to the security, confidentiality, integrity, or availability of any electronic, paper, or other records containing personal or other sensitive information.
    ii. Assess the likelihood and potential damage that could result from such risks, taking into consideration the sensitivity of the personal and other sensitive information.
    iii. Evaluate the sufficiency of relevant policies, procedures, systems, and safeguards in place to control such risks in areas that include, but may not be limited to:
        1. Employee, contractor, and stakeholder training and management;
        2. Employee, contractor, and stakeholder compliance with this WISP and related policies and procedures;
        3. Information systems, including network, computer, and software acquisition, design, implementation, operations, and maintenance, as well as data processing, storage, transmission, retention, and disposal; and
        4. SandBox Union's ability to prevent, detect, and respond to attacks, intrusions, and other security incidents or system failures.

b. Following each risk assessment, SandBox Union will:
    i. Design, implement, and maintain reasonable and appropriate safeguards to minimize identified risks;
    ii. Reasonably and appropriately address any identified gaps.
    iii. Regularly monitor the effectiveness of SandBox Union's safeguards, as specified in this WISP (see Section 8).

5. **INFORMATION SECURITY POLICIES AND PROCEDURES.** As part of this WISP, SandBox Union will develop, maintain, and distribute information security policies and procedures in accordance with applicable laws and standards to relevant employees, contractors, and other stakeholders to:

a. Establish policies regarding:
    i. Information classification (see SandBox Union Information Classification Policy);
    ii. Information handling practices for personal and other sensitive information, including the storage, access, disposal, and external transfer or transportation of personal and other sensitive information;

iii. User access management, including identification and authentication;
iv. Encryption;
v. Computer and network security;
vi. Physical security;
vii. Incident reporting and response;
viii. Employee and contractor use of technology, including Acceptable Use and Bring Your Own Device to Work (BYOD);
ix. Secure coding standards; and
x. Information systems acquisition, development, operations, and maintenance.

b. Detail the implementation and maintenance of SandBox Union's administrative, technical, and physical safeguards (see Section 6).

6. SAFEGUARDS.

SandBox Union will develop, implement, and maintain reasonable administrative, technical, and physical safeguards in accordance with applicable laws and standards to protect the security, confidentiality, integrity, and availability of personal or other sensitive information that SandBox Union owns or maintains on behalf of others.

a. Safeguards shall be appropriate to SandBox Union's size, scope, and business; its available resources; and the amount of personal and other sensitive information that SandBox Union owns or maintains on behalf of others while recognizing the need to protect both customer and employee information.

b. SandBox Union shall document its administrative, technical, and physical safeguards in SandBox Union's information security policies and procedures (see Section 5).

c. SandBox Union's administrative safeguards shall include, at a minimum:
i. Designating one or more employees to coordinate the information security program (see Section 3);
ii. Identifying reasonably foreseeable internal and external risks and assessing whether existing safeguards adequately control the identified risks (see Section 4);
iii. Training employees in security program practices and procedures, with management oversight (see Section 3);
iv. Selecting service providers that are capable of maintaining appropriate safeguards and requiring service providers to maintain safeguards by contract (see Section 7); and
v. Adjusting the information security program in light of business changes or new circumstances (see Section 11);

d. SandBox Union's technical safeguards shall include maintenance of a security system covering local networks and publicly facing production networks that, at a minimum, support:

i. Secure user authentication protocols, including:

1. Controlling user identification and authentication with a reasonably secure method of assigning and selecting passwords or by using other technologies;
2. Restricting access to active users and active user accounts only, including preventing terminated employees or contractors from accessing systems or records; and
3. Blocking access to a particular user identifier after multiple unsuccessful attempts to gain access or placing limitations on access for the particular system.

ii. Secure access control measures, including:
1. Restricting access to records and files containing personal or other sensitive information to those with a need to know to perform their duties;
2. Assigning access and permissions based on the principle of least privilege; and
3. Assigning unique identifiers and passwords to each individual with computer or network access that are reasonably designed to maintain security.

iii. Encryption of all personal or other sensitive information in transit or at rest.

iv. Reasonable system monitoring for preventing, detecting, and responding to unauthorized use of or access to personal or other sensitive information or other attacks or system failures.

v. Reasonably current network protection for systems that may contain or provide access to systems that may contain personal or other sensitive information

vi. Reasonably current software patches for systems that may contain or provide access to systems that may contain personal or other sensitive information

vii. Reasonably current system security software that (1) includes malicious software protection with reasonably current patches and malware definitions and (2) is configured to receive updates on a regular basis.

e. SandBox Union's physical safeguards shall, at a minimum, provide for the following:

i. Defining and implementing reasonable physical security measures to protect areas where personal or other sensitive information may be accessed, including reasonably restricting physical access and storing records containing personal or other sensitive information in locked facilities, areas, or containers.

ii. Preventing, detecting, and responding to intrusions or unauthorized access to personal or other sensitive information, including during or after data collection, transportation, or disposal.

iii. Secure disposal or destruction of personal or other sensitive information, whether in paper or electronic form, when it is no longer to be retained in accordance with applicable laws or accepted standards

7. **SERVICE PROVIDER OVERSIGHT.** SandBox Union will oversee each of its service providers that may have access to or otherwise create, collect, use, or maintain personal or other sensitive information on its behalf by:

a. Evaluating the service provider's ability to implement and maintain appropriate security measures consistent with this WISP and all applicable laws and SandBox Union's obligations.

b. Requiring the service provider by contract to implement and maintain reasonable security measures consistent with this WISP and all applicable laws and SandBox Union's obligations.

c. Monitoring and auditing the service provider's performance to verify compliance with this WISP and all applicable laws and SandBox Union's obligations.

8. **MONITORING.** SandBox Union will regularly test and monitor the implementation and effectiveness of its information security program to ensure that it is operating in a manner reasonably calculated to prevent unauthorized access to or use of personal or other sensitive information. SandBox Union shall reasonably and appropriately address any identified gaps.

9. **INCIDENT RESPONSE.** SandBox Union will establish and maintain policies and procedures regarding information security incident response (see Section 5). Such procedures shall include the following:

a. Documenting the response to any security incident or event that involves a breach of security;

b. Performing a post-incident review of events and actions taken

c. Notifying customers whose data was involved in an information security incident; and

d. Reasonably and appropriately addressing any identified gaps.

10. **ENFORCEMENT.** Violations of this WISP will result in disciplinary action in accordance with SandBox Union's information security policies and procedures and human resources policies. Please see HR Policies for details regarding SandBox Union's disciplinary process.

11. **PROGRAM REVIEW.** SandBox Union will review this WISP and the security measures defined herein annually, or whenever there is a material change in SandBox Union's business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal or other sensitive information, following a PDCA cycle.

a. SandBox Union shall retain documentation regarding any such program review, including any identified gaps and action plans.

12. **REVISION HISTORY**

Version	Author	Description
1.0	Joseph Organisciak	Policy was approved by management.

Status:	Published
Published:	01/23/2021
Last Reviewed:	04/26/2023
Last Updated:	01/23/2021
Version:	1.0