SECURITY INCIDENT RESPONSE PLAN

Version 6
Last Updated October 23, 2023
# Table of Contents

- Revisions History .................................................................................................................. 3
- Purpose .................................................................................................................................. 4
- Definitions ............................................................................................................................. 4
  - IT Security Incident ("incident") ......................................................................................... 4
  - Playbooks ........................................................................................................................... 4
- Risk Assessment Classification Matrix .................................................................................. 5
- Internal / Insider Threat Countermeasures ........................................................................... 7
- Incident Identification and Response ..................................................................................... 8
- HSX Identified Security Issue ............................................................................................... 8
- Individuals Complaints ......................................................................................................... 9
- Employee and Contractor Disciplinary Process ................................................................... 10
- HSX Cyber Insurance .......................................................................................................... 10
- NextGen Incident Response Program Summary ................................................................. 11
- NextGen Identified Security Issue ....................................................................................... 12
- AI Incident Response Program Summary ............................................................................ 12
- HSX Incident Response Team ............................................................................................. 18
  - Key Incident Management ................................................................................................. 18
- Incident Classification ......................................................................................................... 19
- Incident Response Playbooks ............................................................................................. 20
  - Triage Phase ...................................................................................................................... 20
  - Response Phase ................................................................................................................. 20
    - Technical Response ........................................................................................................ 20
    - Management Response .................................................................................................. 21
    - Communications Response ............................................................................................ 21
    - Legal Response .............................................................................................................. 21
- Incident Closing .................................................................................................................... 21
- Incident Response Testing .................................................................................................... 22
- Footnotes to Risk Assessment Matrix .................................................................................. 22
- Ransomware Protection: ...................................................................................................... 22
  - NextGen (Direct, Connect, Results, Match) ..................................................................... 22
## Revisions History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version/Section</th>
<th>Revision</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/29/2016</td>
<td>1</td>
<td>Final Approved Plan</td>
<td>Hal Augustine</td>
</tr>
<tr>
<td>5/19/2017</td>
<td>2 / page 7 and 8 – “Insider Threat Countermeasures” Section</td>
<td>Revisions added for HITRUST Domain 15.07 to incorporate documentation of insider threat countermeasures.</td>
<td>Hal Augustine</td>
</tr>
<tr>
<td>11/18/2019</td>
<td>3 / risks</td>
<td>Refined risk rating</td>
<td>Hal Augustine</td>
</tr>
<tr>
<td>12/12/2021</td>
<td>4</td>
<td>HITRUST for control0162.04b1Organizational.2</td>
<td>Hal Augustine</td>
</tr>
<tr>
<td>1/13/2022</td>
<td>5</td>
<td>HITRUST For control 1311 adding crisis management testing</td>
<td>Hal Augustine</td>
</tr>
<tr>
<td>10/23/2023</td>
<td>6</td>
<td>Removed ACF and CAH and added Panels on page 5. Replaced “Mirth” with “NextGen” removed Diameter</td>
<td>Hal Augustine</td>
</tr>
</tbody>
</table>
Purpose

The HealthShare Exchange of Southeastern Pennsylvania (HSX) IT Security Incident Response Plan is established to protect the integrity, availability and confidentiality of protected health information and confidential or proprietary information, to prevent loss of service and to comply with legal requirements. This plan establishes the coordination of HSX’s response to computerized and electronic communication systems incidents to enable quicker containment, remediation and reporting.

This plan governs HSX general response and subordinate procedures for documentation, tracking, responding to and reporting of incidents affecting computerized and electronic communication information resources, such as theft, intrusion, misuse of data, other activities contrary to HSX’s acceptable use policy, data misuse policy, denial of service, corruption of software, computer and electronic communication-based HIPAA violations, and incidents reported to HSX by other institutions and business entities. It also highlights the necessary collaboration between HSX and its covered entities in incident responses.

Given the HSX infrastructure and security technology tools are cloud-based and are largely managed through Vendor relationships, his plan further establishes dependencies, collaboration and coordination points with HSX Vendors (NextGen and Ai).

The HSX Management team should set and communicate reasonable timeframes for the investigation and response to any security incident based upon its understanding of complexity, response actions required, dependencies on its vendors and other external support resources, and its past experience.

HSX shall provide education to its staff in the agreed procedures and processes, including crisis management. HSX shall test the employee’s knowledge of the plan annually.

Definitions

**IT Security Incident (“incident”)** is any activity that harms or represents a serious threat to the whole or part of HSX’s information assets and infrastructure, such that there is an absence of service, inhibition of functioning assets, unauthorized exposure, change or deletion of critical data assets.

**Playbooks** are used to document the appropriate incident response team participants, resources, the “escalation” of contacts within HSX, its membership, participants and Vendors, and determine those procedures applicable for each class of
incident including communications. These playbooks provide HSX leadership and response teams with guidance in the event of a security incident requiring immediate response to assess, contain, minimize and repair the impact of any anticipated threat.

**Risk Assessment Classification Matrix**

HSX has established a risk assessment classification matrix for its services and information assets. The objective of this assessment is to identify potential security incident threats and determine which HSX services, if any, are at risk for each threat. This information allows HSX to focus its’ response to each incident through the development of “playbooks” to address each likely risk. The risk assessment shall identify the Likelihood of the risk and Impact the risk would have should it occur. These are expressed in each cell below (Likelihood / Impact). HSX shall update this risk assessment as new services and information assets are deployed, and update playbooks whenever deemed necessary. The table below provides the results of that assessment. For the purpose of this risk assessment, the “Direct” column includes Webmail and XDR Mail.

The ratings are color coded to bring focus to each threat type and service in terms of likelihood and risk, and therefore to set priorities for development of incident response playbooks. Legend:

- **.Red** – High Priority
- **.Yellow** – Moderate Priority
- **Green** – Low Priority

<table>
<thead>
<tr>
<th>Security Threat Type</th>
<th>CDR</th>
<th>Direct</th>
<th>ENS</th>
<th>PD</th>
<th>Panels</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internal /Insider</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I.1 Incidental Disclosure</td>
<td>DP:M/</td>
<td>L/L</td>
<td>L/M</td>
<td>L/M</td>
<td>L/M</td>
</tr>
<tr>
<td>XDS:L/ M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I.2 Inappropriate privileged user access or actions by a disgruntled employee, intern or consultant resulting in:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2.1 Unauthorized use or disclosure of HSX information assets</td>
<td>L/H</td>
<td>L/M</td>
<td>M/M</td>
<td>L/L</td>
<td>M/M</td>
</tr>
<tr>
<td>1.2.2 Intentional Service disruption</td>
<td>L/H</td>
<td>L/H</td>
<td>L/H</td>
<td>L/L</td>
<td>L/H</td>
</tr>
<tr>
<td>1.2.3 Intentional deletion or changed information assets</td>
<td>L/H</td>
<td>L/M</td>
<td>L/H</td>
<td>L/L</td>
<td>L/H</td>
</tr>
<tr>
<td>I.3 Identification of unauthorized access (e.g., shared access credentials, unauthorized /</td>
<td>DP: M/</td>
<td>L/M</td>
<td>L/M</td>
<td>L/M</td>
<td>L/M</td>
</tr>
<tr>
<td>XDS:L/ M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Threat Type</td>
<td>CDR</td>
<td>Direct</td>
<td>ENS</td>
<td>PD</td>
<td>Panels</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------------</td>
<td>-----</td>
<td>--------</td>
<td>-----</td>
<td>----</td>
<td>--------</td>
</tr>
<tr>
<td>inappropriate access credentials, internal hacking</td>
<td>L/L</td>
<td>L/L</td>
<td>L/L</td>
<td>L/L</td>
<td>L/L</td>
</tr>
<tr>
<td>I.4 Lost / stolen HSX Laptop</td>
<td>L/L</td>
<td>L/L</td>
<td>L/L</td>
<td>L/L</td>
<td>L/L</td>
</tr>
<tr>
<td>I.5 Loss of a personal device with access to HSX information assets (e.g., stored</td>
<td>L/L</td>
<td>L/L</td>
<td>L/L</td>
<td>L/L</td>
<td>L/L</td>
</tr>
<tr>
<td>credentials for access to email, Onedrive, etc.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I.6 Confidential documents physically missing</td>
<td>L/L</td>
<td>L/L</td>
<td>L/L</td>
<td>L/L</td>
<td>L/L</td>
</tr>
<tr>
<td>I.7 Office burglary</td>
<td>L/L</td>
<td>L/L</td>
<td>L/L</td>
<td>L/L</td>
<td>L/L</td>
</tr>
<tr>
<td>I.8 Phishing / Spoofing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**External**

| E.1 Ransomware¹                                                                       | L/L | L/L    | M/L | M/L| M/L    |
| E.2 Intrusion Detection System or SIEM alert / notification                          | L/M | L/M    | L/M | L/M| L/M    |
| E.3 Bot                                                                              | L/M | L/M    | L/M | L/M| L/M    |
| E.4 Virus                                                                            | L/H | L/H    | L/H | L/L| L/H    |
| E.5 Phishing / Spoofing                                                              | L/H | L/H    | L/H | L/L| L/H    |
| E.6 Inappropriate privileged user access or actions resulting in:                   |     |        |     |    |        |
| E.6.1 Unauthorized use or disclosure of HSX information assets                      | M/L | L/L    | M/M | L/L| M/L    |
| E.6.2 Intentional deletion or changed information assets                             | L/M | L/L    | L/M | L/L| L/M    |
| E.7 Member Breach                                                                    | L/H | L/H    | L/H | L/L| L/H    |
| E.8 Participant Breach                                                               | L/H | L/H    | L/H | L/L| L/H    |
| E.9 Vendor Breach (e.g., NextGen, Ai, Stella, Consultant)                           | L/H | L/H    | L/H | L/ H| L/H    |
| E.10 Social Engineering                                                              | L/H | L/H    | L/H | L/ H| L/H    |
**Internal / Insider Threat Countermeasures**

Due to the complexity associated with Internal security threats, HSX shall evaluate risks and implement reasonable countermeasures to minimize and contain potential security incident occurrences prior to adverse business impact. As such, HSX has identified and implemented the following countermeasures to be reviewed annually and updated as may be necessary:

<table>
<thead>
<tr>
<th>Counter Measure</th>
<th>HSX Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Education / Awareness: Promoting Insider Threat Awareness training that educates employees, interns and contractors of what is considered insider crimes, the consequences and their responsibility to report.</td>
<td>HSX shall implement and maintain training for employees, interns and contractors through training on HIPAA, HSX Policies and Security Training as per the HSX Privacy and Security Awareness Training Policy.</td>
</tr>
<tr>
<td>Accountability: Holding employees, interns and contractors responsible for their actions that jeopardize the confidentiality, integrity and availability of services and information assets.</td>
<td>HSX has developed, approved and implemented policies covering Termination, Data Misuse, Sanctions and Disciplinary Policy among other privacy and security policies. HSX management has ensured that employees, interns and contractors are aware of the policies, understand them and have access to all HSX policies.</td>
</tr>
<tr>
<td>Audit Logging: Enabling electronic logs on high risk systems to provide documentary evidence of the sequence of activities that have affected services or information assets at any specific time that an event has occurred.</td>
<td>HSX and its partners have implemented the appropriate logs for applications, networks and Security Information Event Management. NextGen maintains and manages logs for all NextGen networks and services within their cloud. Ai maintains and manages logs for Ai networks and services within their cloud. AWS maintains logs for Services on AWS networks and services within their cloud; however, these logs are managed by HSX technical operations staff.</td>
</tr>
<tr>
<td>Detection and Prevention:</td>
<td>NextGen, Ai and AWS have implemented Intrusion Detection and Intrusion Prevention Systems, which cover all HSX</td>
</tr>
</tbody>
</table>
### Counter Measure

<table>
<thead>
<tr>
<th>Counter Measure</th>
<th>HSX Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementing controls that identify, alert, prevent and report real time activities that pose a risk to HSX services and information assets.</td>
<td>mission critical services. Each of these HSX business partners maintain managed security policies and configurations.</td>
</tr>
<tr>
<td>Active Monitoring: Implementing security solutions to detect and report insider attack before meaningful business impact occurs.</td>
<td>HSX has contracted and implemented the Protenus solution for application / user level only (user behavior analytics and alerts. NextGen, Ai and AWS by contract are required to maintain operations centers to actively monitor and manage event alerts and report incidents to HSX.</td>
</tr>
</tbody>
</table>

### Incident Identification and Response

#### HSX Identified Security Issue

In the event that HSX discovers or is made aware of an incident or believes it may be under attack, HSX will take the following steps high-level steps to assess, prevent, contain and remediate:

- Triage the incident and notify HSX management.
- Assess if channels or services need to be stopped, if configuration change is required, or appliances/servers need to be taken down and take necessary action.
- In the event that no management are available for notification, guidance or approval of options, and it is believed that there is a critical factor that requires immediate action, the most senior HSX staff available is authorized to take any actions deemed to be required, including but not limited to stopping channels, services or shutting down appliances and servers. Such actions must consider the preservation of as much of the environment as possible to support further investigation.
- If a NextGen related incident, contact NextGen Support via Security@Nextgen.com and also direct call to NextGen CISO to coordinate response actions.
- If an Ai related incident, contact Ai Support via email address and directly call to Ai CISO to coordinate response actions.
- Notify and maintain communications with HSX CISO, HSX Privacy Officer, HSX Executive Director.
- Execute incident response actions guided by HSX Incident Response Plan and incident response playbooks.
• HSX shall ensure that information protection programs do not apply safeguards unnecessarily (e.g un-identified information)
• HSX CISO assumes point for HSX’s response team and point for engagement with NextGen security team.
• HSX CISO maintains open communications on current state, strategies, findings, prevention and containment plans.
• HSX Executive Director, HSX Privacy Officer or HSX CISO engages HSX legal consultant for guidance throughout the response.
• HSX Executive Director executes HSX Incident response communications protocols with board, membership and participants, committees and HSX staff, interns and consultants and media as appropriate.
• HSX CISO acquires and maintains documentation of incident description, research, findings, incident response and state of any residual effects.
• HSX Privacy Officer determines if there was a breach and whether or not it was reportable in accordance with HITECH and HSX policies, including engaging legal support for research and guidance.
• HSX Privacy Officer takes appropriate actions in accordance with the HSX Business Associate Agreement.
• Reports and communications shall be made without unreasonable delay and no later than 60 days after the discovery of a security incident, unless otherwise stated by law enforcement orally or in writing, according to the Incident Response Communication Plan in accordance with the HSX agreements. If the statement is made in writing, the notification is delayed for the time specified by the official.
• Incident reports shall include a description of the event, the date of the breach and date of discovery, a description of the types of information involved, recommended steps for individuals or organizations affected by the incident, the steps the organization has or will take to address the incident or breach, and organizational point of contact information.

Individuals Complaints

Individuals may make complaints concerning the information security policies and procedures or the organization's compliance with the policies and procedures. All complaints and requests for changes are documented, along with their disposition, if any. Such complaints may be made directly to their manager or anyone else in management or Human resources. Additionally, complaints may be made anonymously:
  • Anonymous reporting
    o https://www.surveymonkey.com/r/HSXsecurity
    o Password: HSXsecurity701
Employee and Contractor Disciplinary Process:

Failure to comply with policies and procedures shall result in disciplinary action. HSX shall employ a formal disciplinary process for employees, interns and contractors who fail to comply. Such disciplinary process will vary depending on the severity of the failure to comply as determined by the HSX CISO and Director of Human or an appointee as determined by the Director of Human resources. The potential sanctions resulting from the disciplinary process shall include, but are not limited to:

- Remedial training
- Informal counseling
- Formal counseling
- Suspension or removal of access rights to HSX information assets
- Performance evaluation impacts and documentation
- Suspension or rescinding of promotion.
- Transfer from current job position
- Termination of employment with HSX.
- Termination of contracts with Vendors

- The Director, Human Resources shall:
  - support the discipline of employees and/or contractors involved in security incidents.
  - maintain a list of employees and contractors involved in security incidents including the outcome of the investigation.

- If a failure to comply has been alleged to have occurred but prior to the result of the disciplinary process, in cases where the Chief Information Security Officer (CISO) determines that allowing employees and contractors to retain access rights to HSX information assets presents an unacceptable risk to HSX, access rights to HSX information assets may temporarily be suspended.

- In cases where civil or criminal charges are involved, the CISO shall work together with the Director, Human Resources and HSX Legal Counsel where appropriate to determine and take appropriate legal action.

HSX Cyber Insurance

HSX maintains Cyber insurance with CNA (Columbia Casualty Company):

- Insurance Contract 596635346
- CNA Customer Number 629710

CNA – Claims Reporting
P.O. Box 8317
Chicago, IL 60680-8317
Fax: 866-773-7504
Email: SpecialtyNewLoss@cna.com
HSX, as a condition precedent to the obligations of the Insurer shall give written notice of any Claim, Extortion Demand or Privacy Event to the Insurer as soon as reasonably practicable after HSX’ Executive Officer or their designee learns of such Claim, Extortion Demand, Privacy Event or Privacy Regulation Investigation. HSX legal support should be engaged prior to reporting incident to Cyber insurance.

**NextGen Incident Response Program Summary**
NextGen has deployed CISCO’s Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) to identify, prevent and contain any detectable intrusion. NextGen further subscribes to CISCO’s Global Correlation service where new detection and protection rules are dynamically and timely pushed to NextGen’s system as new threats are identified around the globe.

NextGen is contracted with Mandiant/Fireye on retainer for incident response and forensic research. Additionally, NextGen utilizes Mandiant/Fireye to support table-top testing of departmental playbooks detailing procedures to follow in the event of an incident. Each department is responsible for maintaining their “playbook” documenting the appropriate response protocols and detailed steps for various types of incidents. NextGen utilizes Mandiant/Fireye to test their incident response plan annually. This testing is performed in two phases:

- Phase one is a review of the playbooks for appropriateness and completeness.
- Phase two is a scenario based table-top test where participants are required to use their playbooks as a guide to responding to a set of progressive scenarios. Playbooks are revised based upon table top test findings and recommendations from Mandiant/Fireye.

NextGen’s playbooks also include pre-written communications for different scenarios and are supported by media consultants to ensure effectiveness and appropriateness of communications.

NextGen has also deployed technology where certain attacks will cause all channels to route to an external server where they are validated prior to routing back to NextGen standard infrastructure for HSX processing. Suspicious activity is not routed through the NextGen environment. Additionally, the IDS/IPS may also shut down a router based on rules related to unusual traffic.

NextGen is proactive in staying current on new threats and researches them to determine if there is potential for exposure within its environment. Additionally, NextGen CISO has scheduled bi-weekly conference calls with FBI representatives where the latest threats are shared, which are also investigated for potential exposure within NextGen’s environment.
The NextGen CISO tracks and reports on all security tickets. NextGen executives receive a quarterly report and the board of directors receives semi-annual reports.

**NextGen Identified Security Issue**

**IDS/IPS Alerts or Customer Notifications**

NextGen network engineers are notified as soon as a suspected issue/incident alert is reported either by NextGen’s IDS/IPS or a customer notification of an incident or potential incident. The following are the steps that NextGen follows:

- NextGen support open an internal security ticket and responds to a questionnaire (decision tree) that assists in determining if the incident is reportable.
- NextGen CISO and security team is notified and they assume control of the incident response and related actions.
- Egress and inbound logs are checked for unusual traffic.
- Shut down all interfaces and stop all traffic during the research period.
- HSX is notified of a suspected issue and open communications are maintained.
- If NextGen cannot determine what happened or the extent of what happened, Mandiant/Fireye is immediately engaged for forensic research.
- Appropriate actions are identified and taken.
- If NextGen CISO determines it to be a reportable incident, it is reported immediately to OCR.

**Ai Incident Response Program Summary**

**Policy**

In the event that a serious incident or concerning event is determined to have occurred, PSO shall also coordinate with the PSO at each customer organization to provide applicable reports to the participating organization(s), user(s), healthcare consumer(s), and federal and state authorities, as appropriate. Ai shall document and maintain an internal report of the incident, investigation, remediation plan, and any suspension/reinstatement actions taken.

**Procedure**

The Ai Privacy and Security Officer (PSO) will oversee the process by which Ai employees and contractors report and document potential incidents. The PSO will also oversee the completion and review of Breach Notification Risk Assessment tool (attached to this document). This tool will be used to determine whether or not an incident is a breach, or presents a lower risk.
Identify Risks
Identifying risks associated with critical assets or key business processes is the first step towards preparing an organization for Incident Response. Risk Assessment will be performed regularly to assess the risks associated with all Ai assets. Risk Analysis shall determine Risk analysis a critical asset’s exposure and possible threats. Identifying risks will produce a more effective Incident Response process against security Incidents due to the increased awareness of critical systems.

System Preparation for Incident Response
How is Ai going to prevent (prepare for) security incidents from occurring on systems?
   a. Increase secure audit logging
      i. Ai will use Syslog for audit logging.
      ii. Logs are kept for days. 30 Logs shall be kept, maintained, and reviewed constantly in accordance with Ai’s Access Log Policy. Maintain or build up a system’s defenses
      iii. All systems will remain updated with the most recent software versions. This includes, but is not limited to, installing all Operating System and Application Software updates.
      iv. Any unnecessary or unused services shall be disabled to prevent unnecessary risk or security incidents. Back up critical data and store media securely
      v. The Data Backup Policy is in place to maintain the integrity and availability of sensitive data. Information shall be backed up and stored securely according to the Data Backup Procedure. Educate users/employees about system security
      vi. All users, whether they are an employee, a third party member, or a contractor, must complete mandatory Security Awareness Training before permitted access to a system. In order to maintain the security of company assets, all employees will be required to attend periodic security awareness reviews.

These preparations will occur frequently to continue to safeguard all systems, and the valuable information they process and store.

Network Security Measures
Network Administrators shall be responsible for implementing all network security measures.
   a. Firewalls & Intrusion Detection Systems (IDS); IDS is a
   b. Access Control Lists
      i. Local Account: ACL, ACS Network Topologies
      ii. Ai Network Topology Network Traffic Encryption
      iii. SSH for administrators on systems
      iv. IPSec VPN tunnels for remote connectivity Authentication
      v. Local account passwords are always encrypted
      vi. IPSec, Kerberos

Incident Response Policies and Procedures
Employees shall abide and strictly follow the policies introduced in the Security Policy and in the Employee Handbook.
Any individuals within HSX may make complaints or raise concerns to HSX CISO, HSX Privacy Security Officer or HSX CEO concerning the information security policies and procedures or HSX's compliance with such policies and procedures. These concerns should be communicated whether through meetings or through written concerns sent to the above leadership. HSX CISO shall ensure that all complaints and requests for changes are documented, along with their disposition, if any, and such disposition shall be communicated back to the concerned party that raised the concern or complaint.

Incident Response Team (IRT)
The IRT's mission is to:
- Review Security Incident, and based on the evidence collected, implement an appropriate resolution strategy.
- Record, maintain, and secure all documentation and evidence pertaining to the security incident.
- Protect personal privacy rights established by the law and/or Ai’s company policies.
- Control the incident.
- Maintain the confidentiality of the incident to prevent unnecessary exposure.

Ai shall have an Incident Response Team that will respond to and handle all security incidents that occur within the organization. Ai should provide the Incident Response Team with the following to ensure the most effective process for investigating and handling security incidents:
- Hardware
- Software
- Documentation (forms, reports, procedures, policies)
- Training

The IRT shall meet throughout the year to train and practice for possible future security incidents. In the instance that an IRT member is not available during a security incident, backup IRT members will be available and trained.

Security Incident Detection Phase
This phase will occur when an employee, consultant, or third party with authorized access, has witnessed or detected a security incident. Employees and contractors will be trained to detect and report security incidents during mandatory Security Awareness Training. Employees shall report security incidents as soon as possible to prevent further damage to business assets.

Employees
Complete “incident response” ticket type in Jira and email to Ai’s Security Officer to report the security incident.
a. The Jira ticket should include as much relevant information about the potential incident as possible.
b. The body contents of the email should contain the following details:
   i. Current time & date
   ii. Your full name (Who/what reported the incident)
   iii. Nature of the incident
   iv. When the incident occurred
   v. Hardware and/or software involved
   vi. Your personal contact information, plus any other employee’s contact information who has witnessed the security incident

Technical Project Manager
a. Determine severity of the security incident.
   i. If the security incident is life threatening, call 911.
   ii. Otherwise, open a security report ticket, using the information provided by the employee’s email and attachment.
b. Continue to the next phase, Immediate Response Phase.

Immediate Response Phase
Technical Project Manager
a. Assign the security report ticket to a responsible party. The responsible party shall be determined based on the nature of the security incident and the associated job functionality of the Ai employee. Past experience of handling security incidents will also factor in.
b. Provide the responsible party with the original incident response checklist and any other information regarding the security incident at hand. File all documentation.

Responsible Party
a. Review all relevant information regarding the security incident.
b. Determine the status of the security incident.
   i. If the security incident has been solved, report the completion of security report ticket to RT. In this instance, the ticket will be closed by the Technical Project Manager.
   ii. If the security incident has been verified and not solved, continue to the next phase, Security Incident Investigation Phase.

Security Incident Investigation Phase
Responsible Party
a. Review the security incident. Look for specific details that may help the investigation.
b. Collect the necessary data to resolve the security incident. Data collection is described below. It will provide sufficient details regarding the types of data that may contribute to an investigation. Data can be used as evidence for police reports, legal trials or for disciplinary actions such as employee termination. Contact Network or System administrators in the event of a problem during network or system data collection.
c. Review and analyze collected data. Is the data collected useful for the investigation? Data that is useful to an investigation as evidence should be backed up and stored securely to
prevent tampering or misuse. Backup copies shall be produced according to the Data Back-up Policy.

Data Collection
There are 3 types of data that can be collected during the investigation phase:

a. **System Information**
   The data obtained from a computer or workstation is known as system information. Data collected from a system may be in the form of a log, record, or other document.

b. **Network Information**
   Network information can be collected from the following sources: Firewall logs, Router logs, monitoring logs, Ids logs.

c. **Other Information**
   The collection of data that is not network or system specific is considered "other" information. This includes information and details obtained from employees by means of an old-fashioned, non-technical investigation. Other information may include personnel files and documented interviews with employees and key witnesses. All personnel files and collected data and/or evidence will be secured and documented.

Report Phase
Responsible Party

a. Complete the Incident Response Checklist based on investigation findings and documentation.

b. Submit evidence, incident response checklist, and other relevant findings to the members of the IRT. Include any interviews or research in your documentation.
   i. Documentation should contain:
      - How evidence of the security incident is obtained?
      - Actions taken.
      - Storage location of evidence. Include the method for storing all evidence.
      o Evidence should be tagged and/or labeled

c. Provide the IRT with your contact information. Remain on call in case the IRT needs to discuss the evidence and other relevant information you have obtained during the investigation.

Incident Response Team (IRT)

a. Review and analyze any evidence, checklists, or documentation provided by the responsible party.

b. After a review of the security incident, work with other members in the IRT to decide an appropriate response strategy.
   i. Consider all information obtained throughout the investigation.

c. File the Incident Response Checklist for future reference.

Resolution Phase
The resolution phase is a critical step in the incident response process. The implementation of countermeasures shall restore an organization’s business processes and/or critical systems, while preventing the recurrence of security incidents.

Security Incident resolution should occur in 3 distinct steps:

a. Security Incident Containment
   i. The security incident should be contained prior to any step. Without containment, the security problem could escalate and eventually affect multiple business operations.

b. Security Incident Solution
   i. Once the security incident has been contained, steps should be taken to solve the problem and restore affected systems and business processes.

c. Security Incident Prevention
   i. Steps shall be taken to prevent the recurrence of the security incident. Security policies and procedures should be updated based on new counter measures implemented to protect the organization from future security threats.
   ii. HSX shall perform a cost/benefit analysis for identified countermeasures. Risks classified as low risk and/or low likelihood with high costs may be deferred or risk accepted.

Evidence and data collection should be acquired before any security measures are implemented to prevent altered data.

Follow-up Phase

Incident Response Team (IRT)

a. Review the security report ticket.
   i. Has the incident been resolved or fixed?
      • If the incident has not been resolved/fixed, review security report ticket again. What is missing or what needs to occur to resolve the security incident?
      • If the incident has been resolved/fixed, complete and publish a security report.

b. A Security Report shall contain the following
   i. Executive Summary
   ii. Objectives
   iii. Computer Evidence Analyzed
   iv. Relevant Findings
   v. Supporting Details
   vi. Investigative Leads
   vii. Additional Subsections (Optional)
   viii. Closing Statements/Remarks
   ix. Contact the responsible party to close the security report ticket. Once the ticket has been closed, the requester will receive an email explaining the resolution of the security incident.

c. Root Cause Analysis Form
   i. This will be completed within 2 weeks of the Incident being resolved.
HSX Incident Response Team

HSX incident response team is comprised of HSX, NextGen and Ai resources. The following table presents the parties responsibility assignments.

Key Incident Management:
The CISO shall be the point of contact for coordinating security incident responses.
- Key Incident Management:
  - Brian Wells, CISO 215-796-4622 Brian.Wells@healthshareexchange.org
  - Don Reed, COO/Privacy Officer 484-366-7746 Don.Reed@healthshareexchange.org
  - Martin Lupinetti, CEO 609-792-3896 Martin.Lupinetti@healthshareexchange.org
  - Alice Vuong, Director of IT 267-205-0882. Alice.Vuong@healthshareexchange.org

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>HSX</th>
<th>NextGen</th>
<th>Ai</th>
<th>NextGen Forensics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Manager</td>
<td>CISO</td>
<td>CISO</td>
<td>PSO</td>
<td>Mandiant/Fireye under NextGen Contract</td>
</tr>
<tr>
<td>Management Response Team</td>
<td>CISO and Privacy Officer Executive Director</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Breach Assessment</td>
<td>CISO and Privacy Officer HIPAA Counsel</td>
<td>CISO &amp; Security Team</td>
<td>PSO</td>
<td>Mandiant/Fireye</td>
</tr>
<tr>
<td>Triage Team</td>
<td>Technical Operations Implementation Group</td>
<td>Support Resources</td>
<td>Support Resources</td>
<td>Not likely for this incident type, but if needed: Mandiant/Fireye</td>
</tr>
<tr>
<td>Responsibility</td>
<td>HSX</td>
<td>NextGen</td>
<td>Ai</td>
<td>NextGen Forensics</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------</td>
<td>---------</td>
<td>---------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Technical Response</td>
<td>Program Manager</td>
<td>Security Team</td>
<td>Ai Executive Committee</td>
<td>Mandiant/Fireye</td>
</tr>
<tr>
<td></td>
<td>Technical Ops Lead</td>
<td>Network Engineers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communications</td>
<td>Executive Director</td>
<td>CEO</td>
<td>Ai Executive Committee</td>
<td>Support as needed from Mandiant/Fireye</td>
</tr>
<tr>
<td></td>
<td>Senior Director of Member Relations</td>
<td>Marketing department</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Communications and Marketing Consultant</td>
<td>Media Consultants</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal</td>
<td>HIPAA Counsel</td>
<td>Internal legal team</td>
<td>Internal legal team</td>
<td>Support as needed from Mandiant/Fireye</td>
</tr>
<tr>
<td>Human Resources</td>
<td>HR Manager</td>
<td>Human Resources</td>
<td>Human Resources</td>
<td>Support as needed from Mandiant/Fireye</td>
</tr>
<tr>
<td>Cyber Insurance</td>
<td>Executive Director</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Covered Entities</td>
<td>Executive Director</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Senior Director of Member Services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Covered Entity POC per BAA (documented in Salesforce)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Incident Classification**

The HSX management response team is responsible for classification of the incident based upon available information from the reporting party and the triage team. The management team will then determine the playbook to be followed and direct the response teams.
accordingly. The management team will continue to monitor findings from the incident response teams and is responsible to redirect the response teams if the nature of the security incident is determined to be better addressed through a another playbook.

**Incident Response Playbooks**

Incident response Playbooks, in conjunction with this Incident Response Plan layout the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance with system and information integrity requirements and facilitate the implementation of system and information integrity requirements/controls.

Incident Response Playbooks are developed and maintained for each major HSX area identified with an incident response responsibility. Playbooks may be specific to individual security threat type, or may be developed for a group of security threat types where the incident response is common to those grouped threats. Additionally, playbooks may be written among collaborating groups when such shared playbook is deemed to be more efficient and effective for the response team. Playbooks shall be written and maintained based on agreements reached in facilitated sessions with key stakeholders.

Playbooks shall include, but not limited to, following sections:

**Triage Phase**

This phase is intended to quickly analyze all available information so that security events can be categorized and correlated. This way an organization can most accurately determine the severity and prioritization of events, and assign them to the proper teams for remediation and response. Triage also provides a single point of contact for answering technical questions that arise. The triage process is instrumental for coordinating technical response groups and creating your final response plan. Triage may be dependent on Vendor response teams.

**Response Phase**

This section includes steps taken to address, resolve, or mitigate an incident. During this phase, the incident manager conducts overall response and direction. There are four classes of responses required for an incident:

**Technical Response**

This section is designed to focus on actions taken by technical staff to analyze and resolve an event or incident. Technical staff includes all IT groups required to assist with event or incident remediation, including internal technical staff and external Vendor response teams. It is intended to coordinate and provide technical actions to contain, resolve, or mitigate incidents as well as actions
needed to repair and recover affected systems or data. Additionally, this response team is responsible for maintaining documentation and, where appropriate, maintains chain of custody for related evidence gathered during the response actions.

**Management Response**

This section highlights activities that require any type of management intervention, notification, interaction, escalation, or approval as part of any response. It may include coordinating with legal resources, corporate communications, human resources, public relations, financial accounting, audits, and compliance issues.

**Communications Response**

These activities require communications to the corporation, including internal and external constituents. Corporate communications should always be consulted prior to any statements being released. Additionally, such communications shall be reviewed with HSX executive committee prior to publishing. In the event that time is of the essence and it is not feasible to consult with the executive committee, the HSX executive director or his/her designee may take actions including consult with the board chair or if that is also not feasible release the communication. In many cases, management directs the release of information. This includes issues related to any human resources, public relations, financial accounting, audits, and compliance issues. In the event that a breach has been determined, notifications and reporting must be consistent with regulatory requirements and the HSX Breach Notification policy.

**Legal Response**

This section works with HSX to provide guidance and direction on regulatory requirements and other related legal matters. In addition, their input would be required for any external communications to assure that such communication is in accordance to company policy, Participation and Business Associate Agreements and supports any statutory or regulatory requirements.

**Incident Closing**

After the incident has been contained, eradicated, or mitigated, it is critical to collect all the information available about the incident and conduct an after-incident report. During the incident closing process, the incident team must take steps to properly finalize all documentation, including all analytics and final reports. Additionally, the incident team must take every precaution to preserve all information obtained as part of this process using proper chain-of-evidence procedures, because this information may be required in certain legal responses. After a close-out process is complete, an
incident coordinator conducts a lessons-learned session to identify efficiency improvements in either processes or techniques used for remediation.

**Incident Response Testing**

HSX shall periodically test its security incident response plan as deemed necessary by HSX management team. Prior to any table-top test, HSX CISO and Privacy Officer will appoint a resource to be engaged to identify the testing scope and likely scenarios to be tested. Table-top testing shall occur in two phases similar to NextGen’s testing process:

- **Plan walk-through.** This phase is discussion-based review of the response playbooks where key personnel meet to discuss their roles during an emergency and their responses to a particular emergency situation. It presents an opportunity to validate and refine critical steps and handoffs.

- **Tabletop Scenario-based Exercises.** This phase incorporates facilitation of simulated scenarios where the exercise participants are asked questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination, and decision-making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.

Post table-top test, the testing scenarios, testing results and recommendations for refinement shall be documented and reviewed with HSX management. HSX shall establish a plan for incorporating refinements and monitor to completion within defined timeframes.

**Footnotes to Risk Assessment Matrix**

**Ransomware Protection:**

This section provides information supporting the risk matrix

**NextGen (Direct, Connect, Results, Match)**

NextGen Environment protection from Ransomware: NextGen utilizes a customized Linux-based OS running the appliances and zero Windows systems within that infrastructure, most modern ransomware variants that are in the news today would be unable to launch in that environment. I’m certainly not suggesting Linux will avoid being a target for future variants. The most public variant was Linux Encoder back in 2015. While it is possible to crack the key the hackers used for that malware, it does highlight Linux can be a target.
The NextGen production infrastructure does not have 'shares' in the sense that Windows environments have. This is typically a concern in Windows environments where that type of malware goes on a 'seek and lock' mission attaching itself to any drive (even virtual). NextGen also follows a comprehensive patching program for the underlying OS and there is separation (firewall) between customers.

Finally, the production infrastructure is protected from the NextGen office via a gateway system that leverages ip tables to automate who can access a particular system at any given time. In other words, if an employee’s system was infected within the NextGen office, the malware would not be able to see the production infrastructure.

Ai (ENS Services)
[Requested – pending response]

Rackspace (Provider Directory)
[Pending discussion]