SB Clinical Network, IPA, LLC, d/b/a
Suffolk Care Collaborative

HIPAA Privacy & Security
Policies & Procedures

Adopted by the Board of Directors November 16, 2015
Implemented Fall 2015
Reviewed and revised November 7, 2017
# Suffolk Care Collaborative

## HIPAA Privacy & Security Policies & Procedures

## Table of Contents

<table>
<thead>
<tr>
<th>Policies &amp; Procedures</th>
<th>PDF Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy 1 Commitment to Suffolk PPS Compliance Policies and Procedures</td>
<td>4</td>
</tr>
<tr>
<td>Policy 2 HIPAA Officer Descriptions</td>
<td>5</td>
</tr>
<tr>
<td>Policy 3 Minimum Necessary Use/Disclosure</td>
<td>7</td>
</tr>
<tr>
<td>Policy 4 Workforce Use and Access of Information Systems</td>
<td>10</td>
</tr>
<tr>
<td>Policy 5 ID and Password Assignment for Computer System Access</td>
<td>13</td>
</tr>
<tr>
<td>Policy 6 Network &amp; Remote Access Account Maintenance</td>
<td>16</td>
</tr>
<tr>
<td>Policy 7 Email Usage</td>
<td>18</td>
</tr>
<tr>
<td>Policy 8 Faxing of Protected Health Information (PHI)</td>
<td>21</td>
</tr>
<tr>
<td>Policy 9 Security of Information Technology Resources</td>
<td>23</td>
</tr>
<tr>
<td>Policy 10 Network Infrastructure Access Control and Intrusion Monitoring</td>
<td>25</td>
</tr>
<tr>
<td>Policy 11 Facility Access Control for Electronic Protected Health Information (ePHI)</td>
<td>27</td>
</tr>
<tr>
<td>Policy 12 ePHI Data Backup, Recovery and Testing</td>
<td>29</td>
</tr>
<tr>
<td>Policy 13 Contingency and Disaster Recovery Plan for ePHI</td>
<td>31</td>
</tr>
<tr>
<td>Policy 14 Disposal and Destruction of Paper and Electronic Media</td>
<td>33</td>
</tr>
<tr>
<td>Policy 15 Use of Portable Electronic Devices and Remote Access to Information Systems</td>
<td>34</td>
</tr>
<tr>
<td>Policy 16 Social Media</td>
<td>38</td>
</tr>
<tr>
<td>Policy 17 Subcontractor Business Associate Agreement</td>
<td>41</td>
</tr>
<tr>
<td>Policy 18 Breach Notification</td>
<td>53</td>
</tr>
<tr>
<td>Exhibit A Additional New York State Notification Requirements When Social Security or Financial Information is Included</td>
<td>59</td>
</tr>
<tr>
<td>Exhibit B Risk Assessment Form</td>
<td>60</td>
</tr>
<tr>
<td>Exhibit C Report Form for Potential HIPAA Breaches</td>
<td>61</td>
</tr>
</tbody>
</table>
Policy 19  Monitoring, Activity Review, and Auditing of Information Systems  63
Policy 20  Risk Analysis and Management of PHI  66
Policy 21  HIPAA Training Policy  68
Policy 22  Information Security System and Communication Protection Policy  70
Policy 23  Wireless Networking  73
Policy 24  Multifactor Authentication (MFA) for Access to Identifiable Patient Data via Healthe Intent for DSRIP  75
Policy 25  Policy and Regulatory Violations and Disciplinary Process  78

Appendices

Appendix 1  Electronic Information Access Confidentiality Certification  80
Appendix 2  Sign-In Sheet for SCC DSRIP Systems Access/Use Policy and Procedure Training  83
Appendix 3  User Account Request Form  84
Appendix 4  Information Security Plan  85
COMMITMENT TO SUFFOLK PPS’ COMPLIANCE POLICIES AND PROCEDURES

PURPOSE: SB Clinical Network IPA, LLC, doing business as the Suffolk Care Collaborative performing provider system (the “Suffolk PPS”), recognizes the importance of compliance with the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated by the United States Department of Health and Human Services thereunder (“HIPAA”), and federal and state regulations related to the privacy, confidentiality and security of protected health information, electronic protected health information, and Medicaid Confidential Data. This policy sets forth the commitment on the part of all individuals and entities that participate in or do business with Suffolk PPS, including but not limited to (i) Suffolk PPS and its employees, independent contractors, vendors, agents, suppliers, executives and governing body members; and (ii) all Coalition Partners and their employees, independent contractors, vendors, agents, suppliers, executives and governing body members (“PPS Associates”) to be aware of and conduct themselves in accordance with the standards set forth in Suffolk PPS’ HIPAA compliance policies and procedures for purposes of the Delivery System Reform Incentive Payment (“DSRIP”) program.

POLICY: Suffolk PPS is committed to compliance with federal and state privacy and security requirements and has established thorough HIPAA policies and procedures compliance measures to achieve such commitment. These policies and procedures represent standards of conduct for Suffolk PPS.

1. **Coalition Partners.** Each Coalition Partner is responsible for implementing policies and procedures regarding HIPAA privacy and security internally. Each Coalition Partner is independently responsible for ensuring that its internal employees, independent contractors, agents, executives and governing board members are aware of and comply with such policies and procedures. Suffolk PPS’ HIPAA policies and procedures apply to the participation, conduct and activities of Coalition Partners to the extent their participation, conduct or activities affect PPS operations and the DSRIP Program. Suffolk PPS’ HIPAA policies and procedures are intended to be a resource to ensure that the PPS’ operations comply with all applicable laws and regulations.

2. **Policy Review:** The Information Privacy and Security policies are reviewed annually by the Suffolk PPS’s Information Privacy and Security Officer, or designee. The policies may be amended from time to time at the Suffolk PPS’ discretion.
SUFFOLK CARE COLLABORATIVE

HIPAA OFFICER DESCRIPTIONS

POLICY: SB Clinical Network IPA, LLC, doing business as the Suffolk Care Collaborative performing provider system (the “Suffolk PPS”), has appointed an Information Privacy and Security Officer to oversee the implementation of the policies and procedures necessary for compliance with state and federal regulations, including but not limited to the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated by the United States Department of Health and Human Services thereunder (“HIPAA”).

ROLES:

The Privacy Officer role responsibilities include the development and implementation of the policies and procedures necessary for compliance with HIPAA regulations. Duties include but are not limited to:

- provide guidance related to federal and state privacy protections;
- investigate allegations/complaints of possible HIPAA violations;
- coordinate and supervise the HIPAA training of individuals and entities that participate in or do business with Suffolk PPS, including but not limited to (i) Suffolk PPS and its employees, independent contractors, vendors, agents, suppliers, executives and governing body members; and (ii) all Coalition Partners and their employees, independent contractors, vendors, agents, suppliers, executives and governing body members (collectively, “PPS Affiliates”), for purposes of Suffolk PPS operations and the Delivery System Reform Incentive Payment (“DSRIP”) program;
- assess privacy and/or security risks in collaboration with Suffolk PPS’ Security Officer, and facilitating risk management procedures;
- serve as a liaison to PPS Associates on HIPAA-related issues pertaining to the Suffolk PPS operations and the DSRIP program;
- document and maintain reports of incidents and the steps taken to mitigate such incidents; and
- at a minimum annually review and update all HIPAA related forms and policies.

The Security Officer role responsibilities include oversight, implementation and compliance with the HIPAA Security Regulations, evaluating Suffolk PPS’ risks and implementing measures to secure all electronic protected health information (“e PHI”). Duties include but are not limited to:

- maintain documentation of the Security Officer designations for a minimum period of six (6) years from the time the designation was last in effect;
- conduct/coordinate the periodic Security Risk Analysis and Risk Management/Mitigation process;
- determine appropriate data access level(s) required by PPS Associates,
- document and maintain reports of security incidents and the steps taken to mitigate such incidents;
facilitate updating, testing and maintenance of the Suffolk PPS’ data back-up, recovery and contingency procedures;

oversee the periodic evaluation of Suffolk PPS’ security procedures including but not limited to the implementation of administrative, physical and technical safeguards to ensure Suffolk PPS is applying reasonable efforts to comply with HIPAA Security Rule;

create and maintain an inventory of hardware, software and information systems/applications in order to determine where e-PHI is stored, how it is transmitted, and which PPS Associates (Partners?) currently have access to such systems;

determine the criticality of the data (i.e., how would the loss or short term unavailability of the data impact Suffolk PPS);

make a good faith effort to identify known and/or reasonably anticipated threats to e-PHI and any vulnerability that would cause a program or system to be impacted by such threats; and

at a minimum annually review and update HIPAA security related policies as necessary

PROCEDURE: Suffolk PPS Coalition Partners recognize that they are obligated to appoint a Privacy Officer and Security Officer and provide the contact information of such officers to Suffolk PPS. Such contact information remains on file with Suffolk PPS and each Coalition Partner is responsible for updating such contact information, as needed. Each Coalition Partner’s Privacy Officer is obligated to implement HIPAA policies and procedures applicable to the Coalition Partner for purposes of the DSRIP program. Each Coalition Partner is responsible for implementing such policies and procedures internally. The Coalition Partner is independently responsible for ensuring that its internal employees, independent contractors, executives and governing body members are aware of and comply with such policies and procedures.
SUFFOLK CARE COLLABORATIVE

MINIMUM NECESSARY USE/DISCLOSURE POLICY

PURPOSE: The minimum necessary rule generally requires that, when using, disclosing or requesting protected health information (“PHI”), SB Clinical Network IPA, LLC, doing business as the Suffolk Care Collaborative performing provider system (the “Suffolk PPS”), takes reasonable steps to limit the PHI to the minimum amount necessary to accomplish the intended purpose of the use, disclosure or request.

The minimum necessary rule does not apply to:

1. disclosures to or as requested by a health care provider for treatment purposes after the disclosing party has obtained appropriate assurance(s) that a treatment relationship exists.
2. disclosures to the patient;
3. uses or disclosures made pursuant to a patient authorization;
4. disclosures to the U.S. Department of Health and Human Services when disclosures of patient information are required under the Privacy Rules; or
5. uses or disclosures as required by law.

PROCEDURE:

A. USES OF PATIENT INFORMATION: Suffolk PPS takes reasonable efforts to limit the access of individuals and entities that participate in or do business with Suffolk PPS, including but not limited to (i) Suffolk PPS and its employees, independent contractors, vendors, agents, suppliers, executives and governing body members (“PPS Associates”); and (ii) all Coalition Partners and their employees, independent contractors, vendors, agents, suppliers, executives and governing body members to the minimum necessary identifiable patient information they require for business/operational purposes. Only those individuals with a “need to know” in order to perform their job responsibilities have access to PHI. PPS Associates are specifically instructed that they cannot:

1. access information about themselves, their family members, friends, neighbors, colleagues, co-workers, etc.;
2. access information about celebrities, media personalities, elected officials, or others made famous through media coverage such as accident victims, etc.;
3. discuss with others interesting cases or famous patients, unless there is a job-related reason for doing so;
4. discuss any patient information with family members or friends; or
5. discuss patients in public areas such as elevators, hallways, cafeteria, local coffee shops or other retail locations, etc.

B. ROUTINE OR RECURRING DISCLOSURES OR REQUESTS OF PHI
1. The following measures are required to limit the amount of PHI/e-PHI created, received, disclosed, maintained, transmitted or stored by a requestor to that which is reasonably necessary to achieve the purpose of the disclosure:
   a. isolating and locking file cabinets or records rooms containing PHI;
   b. implementing security requirements/procedures for computers to limit access to PHI;
   c. establishing role based access for electronic PHI;
   d. keeping a logs and/or audit trails of access to electronic patient information;
   e. limiting access to areas handling/storing medical records to authorized individuals only; and
   f. conducting random audits of access to, and requests for, PHI/e-PHI to ensure unauthorized persons are not accessing patient information.

2. Suffolk PPS does not make a detailed determination about the propriety of each and every routine or recurring disclosure. Additionally, Suffolk PPS relies, if reliance is reasonable under the circumstances, on the assumption that a requested disclosure meets the minimum necessary rule in the following circumstances:
   a. requests from Public Officials;
   b. requests from Covered Entities;
   c. requests from professionals who are business associates or subcontractors; and
   d. researchers who proved appropriate representations including but not limited to IRB approval(s), list of approved study personal, documentation of Human Subject training for study personal, data security measures, study collaboration data protection, etc.

3. Suffolk PPS does not disclose an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the disclosure. Since disclosures of PHI made for treatment purposes are exempt from the minimum necessary rule, disclosures of the entire medical record for this purpose are acceptable.

C. NON-ROUTINE/NON-RECURRING DISCLOSURES OF OR REQUESTS FOR PHI: For non-routine or non-recurring disclosures of or requests for PHI, Suffolk PPS reviews each disclosure or request on a case-by-case basis. In addition, each non-routine or non-recurring disclosure of or request for an entire medical record is reviewed on a case-by-case basis. In each instance, Suffolk PPS determines whether the minimum amount of PHI is being disclosed or requested. The criteria which Suffolk PPS considers in evaluating each disclosure or request includes:

1. the purpose of the disclosure/request;
2. the type of patient information to be disclosed or requested (e.g. does it unnecessarily include particularly sensitive information);
3. the minimum amount of patient information necessary to achieve the purpose of the disclosure or request;
4. for disclosures, the amount of patient information requested for disclosure;
5. the individuals/entities to whom a disclosure or request is to be made;
6. the time frame for the disclosure or request; and
7. any specific patient considerations.
D. **ENFORCEMENT**: Suffolk PPS, through its Information Privacy and Security Officers, makes reasonable efforts to limit the access of PPS Associates to only the PHI needed to accomplish job/position related responsibilities. In addition, Suffolk PPS makes reasonable efforts to enforce the minimum necessary rule and the policies described in this policy, through initiatives such as audit and compliance reviews.

E. **Policy Review**: This policy is reviewed at least annually by the Suffolk PPS’s Information Privacy and Security Officer, or designee. This policy may be amended from time to time at the Suffolk PPS’ discretion.

F. **COALITION PARTNERS**: Each Coalition Partner is responsible for implementing such policies and procedures internally. The Coalition Partner is independently responsible for ensuring that its internal employees, independent contractors, executives and governing body members are aware of and comply with such policies and procedures.

G. 3129974 v1
SUFFOLK CARE COLLABORATIVE

POLICY REGARDING WORKFORCE USE AND ACCESS OF INFORMATION SYSTEMS

POLICY: SB Clinical Network IPA, LLC, doing business as the Suffolk Care Collaborative performing provider system (the “Suffolk PPS”), recognizes the importance of training all individuals and entities that participate in or do business with Suffolk PPS, including but not limited to (i) Suffolk PPS and its employees, independent contractors, vendors, agents, suppliers, executives and governing body members (“PPS Associates”); and (ii) all Coalition Partners and their employees, independent contractors, vendors, agents, suppliers, executives and governing body members on the policies and procedures regarding use and access of protected health information (“PHI”) related to the Health Insurance Portability and Accountability Act 1996 and the regulations promulgated by the United States Department of Health and Human Services thereunder (“HIPAA”), the Health Information Technology for Economic and Clinical Health Act 2009 (“HITECH”), and the Suffolk PPS Compliance Code of Conduct.

PROCEDURES:

A. Workforce Confidentiality Agreement. PPS Associates are required to review and sign a confidentiality agreement on an annual basis, pertaining but not limited to the confidentiality of PHI in accordance with HIPAA, HITECH, Suffolk PPS Compliance Code of Conduct, state and federal confidentiality laws for HIV-related, mental health, alcohol and substance abuse treatment and/or genetic information. Individuals breaching the confidentiality requirements of federal or state laws and/or Suffolk PPS policy are subject to appropriate disciplinary actions and/or sanctions.

1. Suffolk PPS confidentiality policies and procedures:
   a. protect the confidentiality of an individual’s PHI;
   b. provide an ongoing reminder to PPS Associates about the importance of confidentiality;
   c. provide for appropriate discipline and/or sanctions, should a breach of confidentiality occur; and
   d. document acknowledgement of a PPS Associate’s responsibilities for protecting confidential health information.

2. New PPS Associates are required to sign a Workforce and Electronic Information Access Confidentiality Acknowledgement Statement (Confidentiality Statement). The signed Confidentiality Statement is filed in the individual’s file and/or electronically recorded in their Human Resources file.
3. PPS Associates are recertified on an annual basis and asked to read and sign a Confidentiality Agreement annually. The signed Confidentiality Statement is filed in the individual’s file and/or electronically recorded in their Human Resources file.

B. **User Access Authorization.** Suffolk PPS ensures the confidentiality, integrity and availability of electronic Protected Health Information (“e-PHI”) by implementing reasonable safeguards (administrative, physical and technical) to prevent unauthorized access to e-PHI while ensuring that properly authorized PPS Associates have proper access to perform their position duties and responsibilities.

1. Only properly authorized PPS Associates and subcontractor business associates have access to e-PHI Systems.

2. Suffolk PPS’ Information Privacy and Security Officer reviews and documents user access rights on a periodic basis and updates the access rights as necessary according to established policies and procedures.

3. Suffolk PPS’ Information Privacy and Security Officer establishes an official documented process for access to e-PHI and e-PHI Systems. This process may include:
   a. identification and definition of permitted access methods;
   b. identification and definition of length of time that access is granted to an individual (e.g., indefinite; a fixed period for temporary engagement; a fixed limited period based on business need);
   c. definition of appropriate tracking and logging of access by authorized users to e-PHI Systems utilizing established oversight monitoring practices and procedures;
   d. a procedure for granting PPS Associate’s access or modifying PPS Associate’s existing access method;
   e. a procedure for managing access rights in a networked and distributed environment, where appropriate, to the e-PHI Systems; and
   f. a procedure to address breaches of the established policies and procedures.

4. PPS Associates are allowed to access only e-PHI that is necessary in order to perform their position duties and responsibilities.

5. Suffolk PPS trains PPS Associates on proper use of access rights. Training is on-going and documented.

6. In accordance with Suffolk PPS employment policies, individuals are screened during the hiring process.

7. In accordance with Suffolk PPS access termination policies, Suffolk PPS implements a documented process for terminating access to e-PHI when a PPS Associate’s employment or affiliation ends and/or when access is no longer necessary.

8. Upon termination/separation of service all mobile and other electronic devices distributed by Suffolk PPS to a PPS Associate for business purposes are returned to individuals designated by
Suffolk PPS to perform Information Technology services ("IT") with keys, ID badge, etc., as appropriate.

C. **Workforce Member Termination/Role Change.** Whenever an individual terminates their employment for any reason or has a significant change in their job function which no longer requires them to have access to buildings, secured areas, physical equipment, and patient information, access is denied for all PPS Associates no longer requiring privileged access. In addition, keys, access cards/badges and other information concerning Suffolk PPS data is returned to Suffolk PPS, as appropriate.

1. Suffolk PPS has a designated individual to perform Human Resources reviews. When he/she knows the date that a PPS Associate is to be:
   
   A. temporarily suspended;
   
   B. terminated;
   
   C. significantly changing his/her job function; or
   
   D. terminating a contractual relationship with Suffolk PPS

2. When the PPS Associate no longer requires their current access status, IT is informed to change or disable access, as appropriate.

3. In the event of an emergency, Suffolk PPS’ Information Privacy and Security Officer (or designee) is contacted and directs appropriate IT staff to immediately disable user accounts and access.

7. Suffolk PPS’ Information Privacy and Security Officer or the individual designated to perform Human Resources reviews updates the PPS Associate’s record to indicate “Electronic Access Suspended”.

E. **Disciplinary Action.** Any member of Suffolk PPS workforce who violates this policy is subject to, disciplinary action in accordance with Suffolk PPS policies and procedures, including termination of employment or contract with Suffolk PPS.

F. **Policy Review:** This policy is reviewed at least annually by the Suffolk PPS’s Information Privacy and Security officer, or designee. This policy may be amended from time to time at the Suffolk PPS’ discretion.

G. **Coalition Partners.** Each Coalition Partner is responsible for implementing policies and procedures regarding workforce use and access of information systems internally. Each Coalition Partner is independently responsible for ensuring that its internal employees, independent contractors, executives and governing board members are aware of and comply with such policies and procedures.
POLICY REGARDING ID AND PASSWORD ASSIGNMENT FOR COMPUTER SYSTEM ACCESS

POLICY: The purpose of this Policy is to protect, limit and control access to the SB Clinical Network IPA, LLC, doing business as the Suffolk Care Collaborative performing provider system (the “Suffolk PPS”), information systems that contain sensitive business information and Electronic Protected Health Information (“e-PHI”).

PROCEDURES: The following guidelines apply to all users of Suffolk PPS Computer systems who are assigned user ID’s and passwords for computer system or network access.

1. **User Accountability.** All users are issued unique user IDs by individuals designated by Suffolk PPS to perform information technology services (“IT”).

2. **Confidentiality.** All affected employees and persons associated with the Suffolk PPS, including executives and governing body members (“PPS Associates”), sign a Workforce & Electronic Information Confidentiality Acknowledgement Statement (Confidentiality Statement) in order to be granted access, honoring all the legal and ethical requirements for protecting and preserving confidentiality and privacy. This includes pre-employment and any subsequent additional requirements or changes in access to PHI either for hard copy or electronic format.

3. **Sharing of User ID/Password.** Sharing of user IDs and passwords is prohibited. With the exception of individuals authorized by Legal Counsel or Human Resources, no PPS Associate is permitted to access another person's accounts.

4. **User Authentication and Access Level.** User Authentication and access is determined by Suffolk PPS and IT on a need to know level based on role. Each user is authenticated by the Suffolk PPS partner using a government issued photo ID, copy of practice license when applicable (MD, RN, etc.) and assignment of a unique Multifactor Authentication (MFA) token for access appropriate to user’s role.

5. **Access.** Access is the ability of an authenticated user to access systems with e-PHI. Methods of access are determined by a unique user name (alternate methods such as biometrics can be used) for identifying and tracking. All passwords consist of a minimum of eight (8) alpha/numeric characters and symbols. Notification regarding password change requirements are sent on a regular basis. System administrator passwords are changed on a regular basis. All users are responsible for their unique user ID and password and to not share or divulge such.
6. **Password Aging.** Passwords are valid for a set period of time for access to clinical or financial systems. Upon expiration of this time period, a new secret password needs to be created by the user. The same password cannot be used within a twelve (12) month time period.

7. **Creation and Modification.** Only authorized IT staff are allowed to create, modify, reset, enable and disable user access to Suffolk PPS Computer Systems. All account activities are logged and audited periodically for appropriateness.

8. **System/Application Log-off.** As per HIPAA Security standards all users are automatically logged off a session if no action is sensed for a defined period of time. This time limit is based upon specific area requirements and approved by IT.

9. **Automatic Log-off.** All system users when logged on to Suffolk PPS’ computer systems (including e-PHI and confidential information systems, etc.) securely disable access or log-off the computer when they are not within close proximity of their workstation to prevent unauthorized persons from using their login to view or access e-PHI or other confidential information. Using another person’s access rights (login ID and Password) to access computer systems is prohibited.

10. **Consecutive Unsuccessful Password Attempts.** User access is disabled after five unsuccessful access attempts with an incorrect password. This policy is to prevent password guessing attacks. In the event the password of an individual becomes disabled, IT can be contacted for a password reset.

11. **Initial Access.** Individuals submit access request forms that have been signed (physical or electronic) by the PPS Associate and that PPS Associate’s supervisor, if applicable. The requestor supplies all information on the access request form. Upon receipt of the request, IT creates a user-id and default passwords for systems requested. The requestor receives email notification of the account and is responsible for notifying the user. Upon first use, the individual is required to agree to comply with the policies and procedures for systems access and to create a unique password with mixed alpha/numeric characters and symbols.

12. **Continued User Access.** The PPS Partner’s designated DSRIP Administrator(s) are required to re-confirm the position/role and continued need for each of their individuals with access to the DOH data on an annual basis.

13. **Subcontractors and Vendors.** Subcontractors and vendors submit access request forms that have been signed by the supervisor responsible for such user access and as per the latest Suffolk PPS Subcontractor Business Associate Agreement. The requestor supplies all information on the access request form which uniquely identifies them. When all information and authorizations are supplied, IT creates a user ID and passwords for the systems requested.

All subcontractor and vendor accounts are valid for up to 60 days or as otherwise requested and approved by Suffolk PPS for a maximum of one year. When access is required beyond one year the requestor validates the need for the Subcontractor/vendor’s continued access annually and promptly notifies the Suffolk PPS’ Information Privacy and Security Officer to discontinue access when the service is complete, contract expires/terminates, sub-contractor/vendor representative is no longer associated with the subcontractor/vendor.
14. **Deleting/disabling User ID's and Passwords.** Access to Suffolk PPS systems is discontinued upon termination of service. For other status changes a request to continue email access for a specified period of time can be submitted to IT for review. Approval is granted on a case-by-case basis. Access including but not limited to clinical information systems, databases, and/or IT reports is disabled for any status change that indicates separation of service from Suffolk PPS.

15. **Monitoring and auditing.** All access and actions performed by the user login "ID" is logged and periodically monitored. Proactive audits are performed to ensure compliance to this policy. Any user posing a significant risk to the systems/applications/organization will have their access disabled within sixty (60) minutes of discovery of the risk. Access audit logs are utilized by the Suffolk PPS Information Privacy and Security Officer as necessary for access investigations.

16. **Policy Review:** This policy is reviewed annually by the Suffolk PPS’ Information Privacy and Security Officer, or designee. This policy may be amended from time to time at the Suffolk PPS’ discretion.

17. **Sanctions.** Attempts to inappropriately access e PHI such as (but not limited to): the use of another person’s login ID and password, and the modification, deletion or use sensitive information/PHI in an unauthorized manner for personal gain or to harm someone is subject to progressive disciplinary measures and/or civil/criminal prosecution.

18. **Coalition Partners.** Each Coalition Partner is responsible for implementing policies and procedures regarding ID and password assignment for computer system access internally. Each Coalition Partner is independently responsible for ensuring that its internal employees, independent contractors, executives and governing board members are aware of and comply with such policies and procedures.
SUFFOLK CARE COLLABORATIVE

POLICY REGARDING NETWORK & REMOTE ACCESS ACCOUNT MAINTENANCE

POLICY: All users accessing SB Clinical Network IPA, LLC, doing business as the Suffolk Care Collaborative performing provider system (the “Suffolk PPS”), network resources and computer application systems have a unique ID and password and Multifactor Authentication (MFA) token. Access for vendors is valid for up to 60 days or as requested for up to one year.

PROCEDURES:

1. **New User Account.**
   a. All new requests for access to Suffolk PPS network resources and Suffolk PPS information computer systems are submitted to the individuals designated by Suffolk PPS to perform information technology services (“IT”).
   
   b. Upon approval, IT (via internal procedures) creates an account and the user and authorized supervisor/designee are notified via email that the request has been completed. IT gives the requester a username and a unique default password to use for initial access. Once the user logs into the network for the first time, he/she is prompted to change the unique default password.
   
   c. A request is then submitted to the appropriate Realm Administrator for MFA token assignment (refer to policy # 24).

2. **Account Changes.**
   a. All requests for changes to access, including but not limited to, access to additional network or computer systems resources or reduction are submitted to the individuals designated by Suffolk PPS to perform information technology services (“IT”).
   
   b. Upon approval, IT provisions the additional access and the user and authorized supervisor/designee are notified via email that the request has been completed and when applicable, IT provides the requester a username and a unique default password to use for initial access. Once the user logs into the network for the first time, he/she is prompted to change the unique default password. For requests to reduce/remove access IT disables the requested access.

3. **Disabling Accounts.**
   a. An authorized supervisor/designee may specifically request that an account be disabled or modified.
b. After the account has been disabled, IT notifies the authorized supervisor/designee.

4. **Network Access and Computer Systems Administration.**
   
   a. Each supervisor is responsible for their employees regarding the proper use and security of network and computer system resources.
   
   b. Access rights are designated by role and functional position responsibilities and are assigned by the supervisor.
   
   c. Supervisors regularly review access to computer systems to ensure appropriate access for position and responsibility and submit account change requests as necessary.

5. **Network Access Violation.** Only persons who have been granted specific authorization through the assignment of a network username and password are allowed to access data via the network and computer systems. All network data can only be accessed and utilized in a manner consistent with the network user's role and position responsibilities.

6. **Policy Review.** This policy is reviewed annually by the Suffolk PPS’ Information Privacy and Security Officer, or designee. This policy may be amended from time to time at the Suffolk PPS’s discretion.

7. **Sanctions.** Individuals who attempt to inappropriately access, modify, delete or use sensitive information or e-PHI are subject to progressive disciplinary measures and/or civil/criminal prosecution.

8. **Coalition Partners.** Each Coalition Partner is responsible for implementing policies and procedures regarding network & remote access account maintenance internally. Each Coalition Partner is independently responsible for ensuring that its internal employees, independent contractors, executives and governing board members are aware of and comply with such policies and procedures.
SUFFOLK CARE COLLABORATIVE

POLICY REGARDING E-MAIL USAGE

POLICY: SB Clinical Network IPA, LLC, doing business as the Suffolk Care Collaborative performing provider system (the “Suffolk PPS”), utilizes secure network electronic mail (“email”) system(s) for approved purposes and in an appropriate manner as defined in the procedures contained in this policy.

PROCEDURES:

1. Email is to be used for Suffolk PPS business purposes and not misused. Email is an efficient way to send urgent messages for those designated to communicate with multiple people simultaneously. All affected employees and persons associated with the PPS, including executives and governing body members will exercise caution to ensure that the correct email address is used for the intended recipient(s).

2. Users must not use an email account assigned to another individual to either send or receive messages, unless the original individual delegates such rights under user access privileges from the users own email account.

3. For security and network maintenance purposes, authorized individuals designated by Suffolk PPS to perform information technology services (“IT”) may monitor equipment, systems and network traffic at any time, in accordance with procedures regarding auditing. Suffolk PPS reserves the right to audit networks and systems on a periodic basis to ensure compliance with this Policy.

4. Individuals should not expect or treat email as confidential or private. Except as permitted by the PPS Lead Organization, no one is permitted to access another person's email. Password sharing is not permitted. Individuals will ensure their unique username and password is secure from other persons. Authorized users are responsible for the security of their passwords and accounts.

5. System users should exercise extreme caution, good judgment and common sense when distributing messages.

6. Confidential operational information must NEVER be disseminated via email outside the individual secure email networks hosted by the PPS partners of the Suffolk Care Collaborative to an unauthorized source(s) (for example yahoo, aol, optonline, gmail, etc.).

7. Protected Health Information (“PHI”) is strictly prohibited from being sent via email outside the secure email networks of the Suffolk PPS to/via another email provider such as AOL, Gmail, Hotmail, a vendor email account or other health system email account. When it is necessary for business purposes to transmit PHI outside the secure email networks of the Suffolk PPS, appropriate IT resources are contacted to arrange secure processes for these communication transmissions. When sending PHI within the secure email networks of the Suffolk PPS, messages will contain only the minimum necessary amount of information needed for the communication or will be completely de-identified.
8. Individuals will abide by copyright laws, ethics rules, quality privilege and other applicable laws.

9. The use of the secure email networks provided by the Suffolk PPS partners to solicit for any purpose without the authorization of the appropriate partner organization CEO or the CEO’s designee is strictly prohibited.

10. Users must be aware that the majority of viruses are transmitted via email. Individuals should not open any attachments or click on any links contained in any suspicious email (spam, phishing attempts) or email from a sender that is not familiar to the email recipient. Appropriate partner’s IT resources should be contacted immediately for further instruction.

11. Sending harassing, abusive, intimidating, discriminatory, or other offensive emails is strictly prohibited. If an individual receives a message containing defamatory, obscene, offensive or harassing information, or that discloses personal information without appropriate permission/authorization, the individual should immediately contact their compliance officer or call the Compliance Helpline and should not delete the message or forward it unless otherwise instructed to by their compliance officer or the Suffolk PPS Compliance Officer.

12. Auto forwarding of official email from one email system to any other email system is not permitted.

13. Emails should contain language similar to the following statement:

   Note: This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by email and destroy all copies of the original.

14. Out of Office auto reply messages must be entered by the account holder. The start and end date/time must be entered to enable this feature. Each account holder can customize the “out of office” message that is received inside the organization and separately to those outside the organization. Automatic replies outside the organization must be selected to enable this feature. Please note the selected start and end date/time is not included in the automatic reply. A start and end date/time must be included in the customized message if the account holder intends to notify the recipient(s) of the “out of office” message this information.

15. Access to a secure Suffolk PPS partner email systems is discontinued upon termination of service.

16. **Retention.** All email is retained until it is moved to trash by the account holder. Emails remaining in trash for an extended period of time will be automatically purged from trash. The account holder may immediately purge emails in trash by emptying trash. Email messages purged from trash will be retained for an additional period of time after their removal to allow recovery by the email systems administrator. After that they will be automatically expunged from the system. Upon request from Legal Counsel, a litigation hold may be placed on the contents of a user’s email account. The hold will cause any held emails which have not been expunged to be retained until the hold is lifted.

17. **Sanctions.** Individuals engaging in the transmission of inappropriate emails or using another user’s ID or password, as determined by Suffolk PPS’s Information Privacy and Security Officer, are
subject to discipline, up to and including termination of employment or contractual relationship with Suffolk PPS.

18. **Policy Review**: This policy is reviewed at least annually by the Suffolk PPS’s Information Privacy and Security Officer, or designee. This policy may be amended from time to time at the Suffolk PPS’s discretion.

19. **Coalition Partners**. Each Coalition Partner is responsible for implementing policies and procedures regarding email usage internally. Each Coalition Partner is independently responsible for ensuring that its internal employees, independent contractors, executives and governing board members are aware of and comply with such policies and procedures.
SUFFOLK CARE COLLABORATIVE

FAXING OF PROTECTED HEALTH INFORMATION

PURPOSE: SB Clinical Network IPA, LLC, doing business as the Suffolk Care Collaborative performing provider system (the “Suffolk PPS”), takes reasonable measures to protect the confidentiality of protected health information (“PHI”) when information is faxed. It is the responsibility of all individuals and entities that participate in or do business with Suffolk PPS, including but not limited to (i) Suffolk PPS and its employees, independent contractors, vendors, agents, suppliers, executives and governing body members (“PPS Associates”); and (ii) all Coalition Partners and their employees, independent contractors, vendors, agents, suppliers, executives and governing body members, to implement reasonable processes to ensure the minimum necessary amount of information is faxed, that the faxed information is received by the intended recipient, that safeguards are in place throughout the faxing process to protect the confidentiality of the faxed information and that all misdirected faxes are reported as potential breaches (refer to policy #18).

PROCEDURES:

1. When it is necessary to fax PHI, using either conventional or electronic faxing capabilities, the person sending the information reviews the content to ensure that only the minimum necessary information is included in the documents to be faxed.

2. A facsimile cover sheet is used whenever PHI is faxed. The cover sheet must not contain any information that identifies the patient(s). The following information is included on the cover sheet:
   a. name, telephone number, and fax number of the person to whom PHI is being sent;
   b. name, address, and telephone number of the person who is sending PHI;
   c. date and time that the fax is being sent;
   d. number of pages being faxed, including the cover page; and
   e. MUST contain a confidentiality notice with language similar to that below (please copy and paste as needed) with an appropriate callback phone number included for notification of a misdirected fax.

CONFIDENTIALITY NOTICE

Document(s) accompanying this facsimile cover sheet contain PRIVILEGED & CONFIDENTIAL information intended solely for the individual or entity to whom it is addressed. If as the READER OF THIS NOTICE you are not the intended recipient, you are hereby notified that any dissemination, distribution or copying of the information accompanying this facsimile cover sheet is STRICTLY PROHIBITED.
If you have received this facsimile in error, PLEASE IMMEDIATELY NOTIFY the HIPAA Privacy Officer by telephone (000) 000 – 0000 to report the error and arrange for proper disposal of the document(s). THANK YOU FOR YOUR ANTICIPATED COOPERATION.

3. All PPS Associates take reasonable measures to ensure that the intended recipient is aware that the information is being faxed and that the faxed information is received by the intended recipient. Telephone confirmation of receipt is required when faxing sensitive information.

4. Upon completion of the faxing process, the original faxed PHI should be properly filed or disposed/destroyed.

5. When PHI is faxed for any purpose other than treatment, payment, or operations, information concerning the fax, including the name, affiliation, and telephone number of the recipient, date and time the faxing occurred, and reason for the fax, is recorded for an accounting of the disclosure or placed in the correspondence section of the medical record for an accounting of the disclosure.

6. To the extent possible, faxing of sensitive information is to be avoided. When sensitive information must be faxed (i.e. urgent, emergency), the sender ensures that confidentiality is maintained. Examples of sensitive information include, but are not limited to information about HIV, mental health, developmental disability, alcohol or drug abuse, sexually transmitted disease, pregnancy results, and genetic screening.

7. Incoming faxes containing PHI are not left on or near any fax machine(s). It is the responsibility of the directors and managers of all work units to implement reasonable processes to ensure incoming faxes containing PHI are distributed promptly to the intended recipient(s) and the confidentiality of the information contain in the fax is maintained.

8. Misdirected faxes containing PHI:
   a. Received by Suffolk PPS are reported to the sender and returned or disposed of as appropriate.
   b. Sent by Suffolk PPS are reported to the HIPAA Information Privacy and Security Officer as part of the breach notification process (refer to policy #18).

9. This policy is reviewed annually by the Suffolk PPS’s Information Privacy and Security Officer, or designee. This policy may be amended from time to time at the Suffolk PPS’ discretion.

10. Each Coalition Partner is responsible for implementing a policy and procedures regarding the faxing of PHI internally. Each Coalition Partner is independently responsible for ensuring that its internal employees, independent contractors, executives and governing body members are aware of and comply with such policies and procedures.
POLICY REGARDING SECURITY OF INFORMATION TECHNOLOGY RESOURCES

POLICY: SB Clinical Network IPA, LLC, doing business as the Suffolk Care Collaborative performing provider system (the “Suffolk PPS”), partners maintain the security of their information systems and applications.

PROCEDURES:

A. Configuration Control. All affected employees and persons associated with the Suffolk PPS, including executives and governing body members are not permitted to install other software packages on their computer workstations without obtaining advanced permission from the individuals designated by Suffolk PPS to perform Information Technology services (“IT”).

B. Changes to Hardware. Computer workstations purchased through the lead organization Stony Brook Medicine IT (IT) are not permitted to be altered in any way (e.g., upgraded processor, expanded memory, or extra circuit boards) without prior authorization from IT.

C. Use of Screen Savers. All Suffolk PPS computer workstations with access to protected health information (“PHI”) are expected to have a screensaver that engages within five (5) minutes of inactivity. Only screen savers approved by IT are installed on Suffolk PPS computer workstations.

D. Virus Protection. All computer workstations run an approved virus detection package, approved by IT.

E. Network Information Gathering Applications. Installation and/or use of networking information gathering applications on computer workstations or server(s) is prohibited unless approved by IT.

F. Modems. Modems are not permitted unless approved by IT.

G. Positioning of Computer Display Screens. Display screens and monitors used to view e-PHI and other confidential, sensitive and/or business related information are positioned such that unauthorized persons cannot easily view the information on the display screen/monitor or have a privacy screen installed on the monitor to minimize over-the-shoulder viewing activity.

H. Use of Personal Equipment. Users are not permitted to bring their own computers, computer peripherals, or computer software into the Suffolk PPS facility without prior authorization from IT.

I. Business Use Only. Suffolk PPS computer workstations and communication systems are used only for Suffolk PPS business related purposes.
J. **Storage, Backup or downloading of e-PHI to Removable Media.** Storing, backing-up or downloading of e-PHI to removable media (CD, USB-drive, portable back-up hard-drive, laptop ,etc.) is strictly prohibited.

K. **Re-authentication.** Unauthorized access to information systems is controlled by implementing authentication or re-authentication after a predetermined period of inactivity for all desktops, laptops, PDA’s and any other computer system that contains PHI or confidential information where authentication is required.

L. **Personal Offices.** Individuals with separate personal offices containing information technology equipment are secured at all times. Unoccupied offices are closed and computer workstations locked or logged-off when unattended.

M. **Server and Communication.** Servers and communications equipment is located in locked limited access locations approved by Suffolk PPS’ Information Privacy and Security Officer, to prevent tampering and unauthorized access/usage. This applies to servers, network switches, PBXs, hubs, routers, firewalls, and other computing and network equipment.

N. **Third Party Access.** Access to secured areas by third parties and other non-authorized employees is supervised and logged (sign-in prior to access and sign-out when leaving the area).

O. **Electronic Media Security.** Information that is confidential/sensitive may be stored on electronic media (such as hard disk and/or portable back-up hard drives, magnetic tapes, CD, USB-drives) if the media is secured through technical safeguards such as encryption and/or physical safeguards such as locked, limited access storage facilities (file cabinet, desk draw, etc.) when not in use or left unattended.

P. **Electronic Devices.** All mobile electronic devices including but not limited to laptops, PDA’s, smart phones, tape, CD/DVD’s and USB devices are password protected and/or encrypted.

Q. **Mobile Device Monitoring.** All mobile devices are equipped with software that allows IT to track and remotely freeze or wipe the device/hard drive when the device is reported lost/stolen.

R. **Termination.** Upon separation or termination from Suffolk PPS computer workstation(s), communications equipment and/or storage media purchased by Suffolk PPS is returned to the applicable supervisor or IT and is not removed from Suffolk PPS premises.

S. **Access Rights to Restricted Areas.** Whenever an individual terminates his or her working relationship with Suffolk PPS, all access rights to restricted areas is promptly revoked.

T. **Policy Review:** This policy is reviewed annually by the Suffolk PPS’ Information Privacy and Security Officer, or designee. This policy may be amended from time to time at the Suffolk PPS’ discretion.

U. **Sanctions.** Individuals who attempt to inappropriately access, modify, delete or use sensitive information or e-PHI are subject to discipline and/or civil/criminal prosecution.

V. **Coalition Partners.** Each Coalition Partner is responsible for implementing policies and procedures regarding security of information technology resources internally. Each Coalition Partner is independently responsible for ensuring that its internal employees, independent contractors, executives and governing board members are aware of and comply with such policies and procedures.
POLICY REGARDING NETWORK INFRASTRUCTURE ACCESS CONTROL AND INTRUSION MONITORING

POLICY: SB Clinical Network IPA, LLC, doing business as the Suffolk Care Collaborative performing provider system (the “Suffolk PPS”), recognizes the importance of implementing technical safeguards to adequately protect confidential information. Suffolk PPS network infrastructure, which has connectivity to the Internet, is protected from unauthorized access with the use of an enterprise-class network firewall(s) and intrusion detection systems (“IDS”).

PROCEDURES:

1. **Applicability.** All firewalls at Suffolk PPS follow this policy. Exceptions from this policy are permitted only if approved in advance in writing by the Suffolk PPS Information Privacy and Security Officer and from the individuals designated by Suffolk PPS to perform Information Technology services (“IT”).

2. **Secured Subnets.** Portions of any Suffolk PPS internal network that contain sensitive or valuable information, including but not limited to the computers used by individuals designated to perform human resources and finance services, systems containing patient information, etc., employ a secured subnet. Access to this and other subnets is restricted with firewalls and other control measures as necessary.

3. **Disclosure of Internal Network Information.** The internal system addresses, configurations and related system design information for all Suffolk PPS networked computer systems is restricted such that both systems and users outside Suffolk PPS internal network cannot access this information. All network equipment requires installation/configuration by or approval from SBMIT Network Services.

4. **Default to Denial for Internet Connectivity.** Every Internet connectivity path and Internet service not permitted and approved by Suffolk PPS’ Information Privacy and Security Officer and IT is blocked by the Suffolk PPS firewalls.

5. **Contingency Planning.** Technical staff working on firewalls prepare and obtain from Suffolk PPS’ Information Privacy and Security Officer and IT approval for contingency plans which address the actions to be taken in the event of various problems including system compromise, system malfunction, and power outage.

6. **Auditing.** Firewalls access logs are monitored on a regular basis and noted/suspected inappropriate activity and/or access to Suffolk PPS networks is promptly reported to Suffolk PPS’ Information Privacy and Security Officer.

7. **Firewall/IDS Configuration Logs.** All changes to firewall and IDS configuration parameters, enabled services, and permitted connectivity are logged and reported on a regular basis to the Suffolk PPS’ Information Privacy and Security Officer and/or IT.
8. **Extended User Authentication.** All approved inbound traffic accessing Suffolk PPS networks through the Suffolk PPS firewall involve extensive user authentication measures approved by IT.

9. **Firewall Modification and Configuration Privileges.** Privilege to modify the functionality, connectivity and services of the firewall is restricted to limited individuals with appropriate authorization. Unless permission from Suffolk PPS’ Information Privacy and Security Officer has been obtained, such privilege is only granted to authorized individuals.

10. **Firewall Physical Security.** Suffolk PPS firewalls are located/situated in locked rooms accessible only to those limited individuals, with appropriate authorization to physical access to such firewalls.

11. **Approval Process.** Before being enabled, all new firewall, IDS services and new connectivity paths are evaluated to determine business advantages and identify security risks. Only IT can either approve or deny such requests. IT is responsible to setup, maintain, and manage the Suffolk PPS firewall.

12. **Administrative Access to Network Devices.** Only individuals designated by Suffolk PPS and IT staff have privileges as administrators of network systems. Suffolk PPS’ Information Privacy and Security Officer, in consultation with IT considers and reviews requests for exceptions to this policy.

13. **Policy Review:** This policy is reviewed annually by the PPS’ Information Privacy and Security Officer, or designee. This policy may be amended from time to time at the Suffolk PPS’ discretion.

14. **Coalition Partners.** Each Coalition Partner is responsible for implementing policies and procedures regarding network infrastructure access control and intrusion monitoring internally. Each Coalition Partner is independently responsible for ensuring that its internal employees, independent contractors, executives and governing board members are aware of and comply with such policies and procedures.
POLICY REGARDING FACILITY ACCESS CONTROL FOR ELECTRONIC PROTECTED HEALTH INFORMATION

POLICY: SB Clinical Network IPA, LLC, doing business as Suffolk Care Collaborative (the “Suffolk PPS”), prevents unauthorized physical access to electronic Protected Health Information (“e-PHI”) systems and the facility in which they are located while taking reasonable steps to ensure that access by properly authorized individuals including but not limited to employees, persons associated with the Suffolk PPS, such as executives and governing body members, is granted.

PROCEDURES:

A. Suffolk PPS protects the confidentiality, integrity and availability of e-PHI by taking reasonable steps to protect e-PHI Systems, as well as the facility in which they are located, from unauthorized physical access, tampering and theft.

B. Suffolk PPS physically locates e-PHI Systems in areas where physical access can be controlled in order to minimize the risk of unauthorized access.

C. Suffolk PPS takes reasonable steps to ensure that the perimeter of the facility containing e-PHI Systems is physically sound, the external walls are properly constructed and the external doors have the appropriate protections against unauthorized access.

D. Physical barriers used to protect against unauthorized entry are extended from the actual floor to the actual ceiling in facilities to prevent against unauthorized access. Doors and windows of all facilities are locked when unattended. External protections, such as window guards or bars, are installed on all windows at ground level and any other windows as reasonably necessary to prevent unauthorized entry.

E. Suffolk PPS takes reasonable steps to ensure that the level of protection provided for the e-PHI Systems, as well as the facility in which they are housed, is commensurate with that of the identified threats and risks to the security of such e-PHI Systems, and its facility as determined by its risk analysis.

F. The risk analysis results indicates areas in the Suffolk PPS facility in which e-PHI Systems are located into documented categories such as:

1. Highly Sensitive - Areas where highly sensitive e-PHI is created, received, transmitted or maintained but only a small, select group of individuals, need access to complete their job duties.

2. Sensitive - Areas where sensitive e-PHI is created, received, transmitted or maintained and a moderately sized group of individuals need access to complete their job duties.

3. Monitoring Required - Areas where large amounts of e-PHI are created, received, transmitted or maintained but a large group of individuals need access to complete their job duties.
G. Suffolk PPS establishes and documents detailed rules to determine which individuals are granted physical access rights to specific areas where e-PHI Systems are maintained on a need-to-know basis.

H. Suffolk PPS reviews and revises physical access rights to areas where e-PHI Systems are maintained on an ongoing basis.

I. All visitors are required to show proper identification (government issued photo ID such as a drivers license or non-drivers identification card or passport) and to sign-in prior to gaining physical access to areas where e-PHI Systems are located and sign-out when leaving the area.

J. Periodic inventory of physical access controls used at the Suffolk PPS facility to protect e-PHI systems are done by the Information Privacy and Security Officer. The inventory report is stored in a secure manner.

K. In accordance with its policy regarding facility security, Suffolk PPS has a facility security plan that details how it protects its facility in which e-PHI Systems are located and equipment from unauthorized physical access, tampering and theft.

L. Suffolk PPS documents repairs and modifications to the physical components, hardware and equipment (that secures, stores, maintains or transmits e-PHI) of its facility that are related to security.

M. Suffolk PPS’s Information Privacy and Security Officer has responsibility for implementation of this policy. Members of Suffolk PPS workforce who violate this policy are subject to disciplinary action in accordance with Suffolk PPS policies and procedures up to and including termination of employment or contract with Suffolk PPS.

N. This policy is reviewed annually by the Suffolk PPS’ Information Privacy and Security Officer, or designee. This policy may be amended from time to time at the Suffolk PPS’ discretion.

O. Each Coalition Partner is responsible for implementing policies and procedures regarding facility access control for e-PHI internally. Each Coalition Partner is independently responsible for ensuring that its internal employees, independent contractors, executives and governing board members are aware of and comply with such policies and procedures.
SUFFOLK CARE COLLABORATIVE

POLICY REGARDING ELECTRONIC PROTECTED HEALTH INFORMATION (e-PHI) DATA BACKUP, RECOVERY AND TESTING

POLICY: The electronic protected health information ("e-PHI") systems are backed up and stored in a secure manner. The Information Privacy and Security Officer of SB Clinical Network IPA, LLC, doing business as the Suffolk Care Collaborative performing provider system (the "Suffolk PPS"), in collaboration with each system administrator, assures each system is regularly backed up, e-PHI is stored in a secure manner, and that testing of backup and restoration procedures is completed.

PROCEDURES:

1. Suffolk PPS performs risk analysis assessments to determine the maximum amount of loss that can occur if the backup of e-PHI and confidential or critical operational information is disrupted. Suffolk PPS uses its risk analysis to determine if the appropriate measures are being implemented to backup e-PHI.

2. The Information Privacy and Security Officer ensures that each system/application administrators implement appropriate backups of e-PHI and confidential and critical operational information systems to create exact and retrievable copies of e-PHI.

3. The Information Privacy and Security Officer ensures that each system/application administrator implements a documented and detailed backup plan for information systems containing confidential, critical operational and e-PHI data.

The backup plan defines the following:

a. person(s) responsible for taking reasonable steps to ensure the backup of confidential, critical operational and e-PHI data in each system;

b. a backup schedule for each system;

c. specifies the confidential, critical operational and e-PHI data systems that are to be backed up;

d. where backup media is to be stored and all affected employees and persons associated with the Suffolk PPS, including executives and governing body members, who may access the stored backup media;

e. where backup media is to be kept secure before it is moved to storage;

f. who may remove the backup media and transfer it to storage;
g. restoration procedures to restore confidential, critical operational and e-PHI data from backup media to the appropriate confidential, critical operational and e-PHI data systems;

4. Confidential, critical operational and e-PHI data systems for which the data backup plan procedures apply, includes: desktops, laptops, networks and servers.

5. The Information Privacy and Security Officer ensures that each system/application administrator implements sufficient backup systems for information systems containing confidential, critical operational and e-PHI data to confirm that exact up-to-date copies of data can be recovered in the event that confidential, critical operational and e-PHI data systems are damaged.

6. The Information Privacy and Security Officer ensures that each system/application administrator tests restoration procedures for information systems containing confidential, critical operational and e-PHI data to confirm the timeliness and effectiveness of those procedures.

7. The Information Privacy and Security Officer ensures that each system/application administrator documents the appropriate retention period for backup media that contains backup copies of confidential, critical operational and e-PHI data.

8. In order to avoid damage from a disaster, backup copies of confidential, critical operational and e-PHI information including complete documentation for restoration are kept in a remote and secure location.

9. Each system/application administrator of confidential, critical operational and e-PHI data systems provides access, to authorized individuals for immediate retrieval of the backup information stored at the remote location in a disaster or emergency.

10. Physical, technical and environmental security requirements for the backup media stored at a remote, secure location should be consistent with the physical and technical security provided for confidential, critical operational and e-PHI data onsite.

11. This policy is reviewed annually by the Suffolk PPS’ Information Privacy and Security Officer, or designee. This policy may be amended from time to time at the Suffolk PPS’s discretion.

12. Each Coalition Partner is responsible for implementing policies and procedures regarding e-PHI data backup, recovery and testing internally. The Coalition Partner is independently responsible for ensuring that its internal employees, independent contractors, executives and governing board members are aware of and comply with such policies and procedures.
POLICY REGARDING CONTINGENCY AND DISASTER RECOVERY PLAN FOR ELECTRONIC PROTECTED HEALTH INFORMATION (e-PHI)

POLICY: SB Clinical Network IPA, LLC, doing business as Suffolk Care Collaborative performing provider system (the “Suffolk PPS”), maintains a current contingency plan to ensure the confidentiality, integrity and availability of electronic Protected Health Information (“e-PHI”). The plan utilizes preventive and recovery controls and processes in order for Suffolk PPS to prepare for and respond to emergencies and/or disasters.

PROCEDURES:

1. Suffolk PPS establishes and implements document emergency response procedures in order to prepare for and respond to emergencies and disasters that may damage e-PHI systems and to take reasonable steps to ensure that critical data can be recovered and can survive a disaster or other emergency.

2. The Contingency Plan includes:

   a. A documented disaster and emergency recovery strategy that aligns with the business objectives and priorities of Suffolk PPS.

   b. A documented data backup plan that aligns with the disaster and emergency recovery strategy.

   c. A documented disaster recovery plan that aligns with the disaster and emergency recovery strategy.

   d. A documented emergency mode operations plan that aligns with the disaster and emergency recovery strategy and is designed to protect the security of e-PHI during and immediately following a disaster or other emergency.

   e. Test, review and revising of policies related to contingency and disaster recovery plan for e-PHI, as needed to ensure effectiveness.

   f. Review and revision of the criticality analysis of e-PHI systems as needed, and how such e-PHI Systems are vulnerable to loss or other damage in the event of a disaster or other emergency.

3. Suffolk PPS provides training about the disaster and emergency response procedures to members of the Suffolk PPS workforce as policies and procedures change. Training is on-going to ensure compliance with this requirement.

4. Suffolk PPS backs up and stores copies of e-PHI.
5. The Suffolk PPS Information Privacy and Security Officer has general responsibility for implementation of this policy. Affected employees and persons associated with the Suffolk PPS, including executives and governing body members who violate this policy are subject to disciplinary action in accordance with Suffolk PPS policies and procedures up to and including termination of employment or contract with Suffolk PPS.

6. This policy is reviewed annually by the Suffolk PPS’ Information Privacy and Security Officer, or designee. This policy may be amended from time to time at the Suffolk PPS’ discretion.

7. Each Coalition Partner is responsible for implementing policies and procedures regarding contingency and disaster recovery plan for e-PHI internally. Each Coalition Partner is independently responsible for ensuring that its internal employees, independent contractors, executives and governing board members are aware of and comply with such policies and procedures.
SUFFOLK CARE COLLABORATIVE

POLICY REGARDING DISPOSAL AND DESTRUCTION OF PAPER AND ELECTRONIC MEDIA

POLICY: SB Clinical Network IPA, LLC, doing business as Suffolk Care Collaborative performing provider system (the “Suffolk PPS”), follows procedures to ensure information maintained in either paper or electronic format (diskettes, data tapes, etc.) is appropriately stored and disposed of in a safe manner without inadvertent/unintentional disclosure of sensitive and/or confidential information, including by not limited to protected health information (“PHI”).

PROCEDURES:

A. Discarding Materials.

1. Lockable, secure containers or cross cut shredders are provided to collect all discarded paper materials at the point of generation.

2. If applicable, affected employees and persons associated with the Suffolk PPS, including executives and governing body members, are shown the location of the locked paper containers in their work area.

3. All paper as well as all items containing PHI and other confidential information including but not limited to folder, binders or CD’s may be deposited. It is not necessary to remove staples or clips.

4. Foodstuff is not allowed in these containers.

5. Only individuals designated by or under contract with Suffolk PPS are permitted to empty the bins, shred and/or bundling the discarded contents. No other individual may handle the materials that have been discarded.

6. The individuals designated by Suffolk PPS empty the bins on a regular schedule however, if the containers become filled to capacity between scheduled pickups, the Suffolk PPS can be contacted to coordinate a non-routine emptying.

7. If an item/object is mistakenly placed in a locked container, the Suffolk PPS can be contacted to make arrangements to have the bin unlocked so the item(s) can be removed.

8. In the event that there is a need to dispose of a large quantity of documents (file purge) or multiple pieces of electronic media containing PHI (CD’s, films, etc.), the Suffolk PPS can be contacted to request oversized, secure bin(s) for a file purge or secure removal of the electronic media. Discarded materials are not to be purged into an office bin to prevent overflow of secure documents.
SUFFOLK CARE COLLABORATIVE

USE OF PORTABLE ELECTRONIC DEVICES AND REMOTE ACCESS TO INFORMATION SYSTEMS

PURPOSE: SB Clinical Network IPA, LLC, doing business as Suffolk Care Collaborative performing provider system (the “Suffolk PPS”), recognizes the importance of establishing security precautions to be used by all affected employees and persons associated with the Suffolk PPS, including executives and governing body members who access or use electronic information systems containing electronic protected health information (“e-PHI”) when using laptops and other portable electronic devices or computers in remote locations.

POLICY: This Policy applies to all individuals using laptop computers and other portable electronic devices (e.g. USB, flash or zip drives, iPads, tablets, smartphones) to access and send e-PHI or other business sensitive information in order to perform job functions. In addition, certain individuals access Suffolk PPS’ information systems remotely from computers located in their homes or offices. Individuals who use laptops or other portable electronic devices or who access e-PHI from external computers are required to take reasonable precautions to protect this equipment from damage or theft and to protect the confidentiality of e-PHI that can be accessed with, or stored on, such devices.

PROCEDURE:

1. **Removal of e-PHI.** The removal or downloading of e-PHI from Suffolk PPS systems is limited to devices provided by the PPS lead organization Stony Brook Medicine Information Technology (SBMIT) or other contracted IT provider(s).

2. **External Hardware:** Collectively, all electronic devices not owned by Suffolk PPS IT provider(s) (but that contain e-PHI that is used for Suffolk PPS purposes) are referred to as (“External Hardware”).
   
   a. Authorized individuals may access the system from remote locations for purposes of performing their job functions (“Permitted Uses”) only. Individuals may only use approved devices to access the system and are prohibited from attempting to access information for reasons other than Permitted Uses.

   b. Use of External Hardware to transmit or receive e-PHI should be limited to that which is absolutely necessary and should be performed in a secure manner (for example using secure file transfer protocol SFTP).

   c. When using External Hardware to transmit or receive e-PHI, or access the system, individuals are required to:

      i. password-protect all External Hardware;
ii. never leave External Hardware unattended while connected to the system;

iii. never leave External Hardware unattended, unless the External Hardware is placed in a secure location;

iv. avoid downloading e-PHI to External Hardware, unless specifically authorized to do so;

v. prohibit unauthorized individuals from using External Hardware if it contains e-PHI or is connected to the system, and avoid using External Hardware to access e-PHI in the presence of others unless for a specific business purpose (while at all times maintaining privacy);

vi. protect the security of External Hardware and the confidentiality of the e-PHI or other business sensitive information contained on it;

vii. immediately report to the Information Privacy and Security Officer any unauthorized use of, or access to, e-PHI; and

viii. keep security software on External Hardware up-to-date.

| d. To the extent practicable, individuals employ automatic screen savers and log-off functions for External Hardware. In addition, if requested by Suffolk PPS, individuals install, or allow for installation of software that allows External Hardware to be wiped clean if it is lost, stolen, or there is otherwise concern for its integrity.

e. To the extent practicable, Suffolk PPS IT provider(s) installs and enables encryption on External Hardware.

f. If the contractual relationship or employment of an individual terminates, or the job duties change such that the use of External Hardware to access e-PHI is no longer appropriate, the individual’s access to the system is terminated.

3. **Portable Devices Distributed by Suffolk PPS.** Portable Device refers to a laptop or other portable device distributed by Suffolk PPS IT provider(s) that contains or could be used to access e-PHI.

a. Portable Devices may be distributed to certain authorized individuals on a temporary or ongoing basis according to job function and management approval. The identification number of the Portable Device and name of recipient is documented and tracked by IT.

b. Portable Devices are to be used by individuals solely for Permitted Uses. Individuals are prohibited from (a) attempting to access information for reasons other than the Permitted Use; or (b) using the Portable Device in any manner beyond the scope of the Permitted Use.

c. While in possession of a Portable Device distributed by Suffolk PPS IT provider(s), individuals are required to:
i. keep the Portable Device in their physical possession at all times and never leave the Portable Device unattended, unless the Portable Device is locked in a secure location;

ii. avoid installing any software or hardware on Portable Device, unless approved by IT; and

iii. prohibit anyone else from using the Portable Device, and avoid using the Portable Device to access e-PHI in the presence of others unless for a Permitted Use (while at all times maintaining privacy).

d. Suffolk PPS protects the security of Portable Devices and the confidentiality of the e-PHI contained on them. e-PHI is never to be stored on the hard drive of a Portable Device.

e. All individuals should avoid accessing the Internet, other than as necessary to access the system or for otherwise Permitted Uses.

f. All individuals have a duty and obligation to immediately report to IT: i) any unauthorized use of, or access to, a Portable Device or e-PHI; ii) any physical damage to the Portable Device; or iii) the loss or theft of the Portable Device. IT immediately reports the issue to the Information Privacy and Security Officer.

g. If a Portable Device, as applicable, is inactive or not in use for more than 15 minutes, the Portable Device automatically goes into a secure mode. To exit out of the secure mode and re-enter the then-current session, individuals need to reenter their password. This does not in any way alter the user’s obligation to log-off and secure any device when leaving the device unattended (refer to section 3 (c) (i), (ii) above.

h. Suffolk PPS IT provider(s):

   i. requires passwords on the Portable Devices;

   ii. installs and enables security software to block unauthorized access to External Hardware; and

   iii. maintains security software on Portable Devices up-to-date.

i. If the contractual relationship or employment of an individual terminates, or the job duties change such that a Portable Device is no longer appropriate, the individual returns the Portable Device to the applicable supervisor or IT.

j. At all times, the Portable Devices remain the property of Suffolk PPS IT provider(s). Individuals are responsible for, and may be liable for, failure to return the Portable Device, report loss in a timely manner, or intentionally causing damage to the Portable Device.

4. Additional Security Measures

   Suffolk PPS IT provider(s) requires mobile device management in the form of an “app” that resides on the mobile device. In the event the mobile device is lost or stolen, Suffolk PPS has the ability to remotely remove all Suffolk PPS data from the device.
5. **Risk Assessment**

   a. As part of the periodic security risk assessments performed by Suffolk PPS, Suffolk PPS considers the potential risks and vulnerabilities associated with Portable Devices and External Hardware and reevaluate risk management measures to reduce such risks and vulnerabilities to a reasonable and appropriate level.

6. **Training**

   a. Individuals are trained regarding the vulnerabilities associated with remote access to e-PHI and Suffolk PPS’ policies and procedures applicable to such use. Training may include instructions for accessing and transmitting e-PHI, password management procedures, rules regarding the downloading of patient data on External Hardware, transmission of e-PHI over open networks, and remote device/media protection. Such training also reinforces policies prohibiting unattended/unsecured Portable Devices and External Hardware and potential sanctions for failing to adhere to policies and procedures regarding laptops, other portable devices and External Hardware.

   b. Suffolk PPS ensures that its affected employees and persons associated with the Suffolk PPS, including executives and governing body members are educated regarding the vulnerabilities associated with remote access and portable devices. Suffolk PPS is responsible for enforcing applicable policies to ensure the safeguard of e-PHI on portable devices. This policy applies to all affected employees and persons associated with the Suffolk PPS, including executives and governing body members. Violations of this policy may result in disciplinary action up to and including termination of employment, contractual relationship with Suffolk PPS or termination of access to the system.

7. **Policy Review**: This policy is reviewed at least annually by the Suffolk PPS’s Information Privacy and Security Officer, or designee. This policy may be amended from time to time at the Suffolk PPS’ discretion.

8. **Coalition Partners**. Each Coalition Partner is responsible for implementing such policies and procedures internally. Each Coalition Partner is independently responsible for ensuring that its internal employees, independent contractors, executives and governing body members are aware of and comply with such policies and procedures.
SUFFOLK CARE COLLABORATIVE

SOCIAL MEDIA POLICY

POLICY: SB Clinical Network IPA, LLC, doing business as Suffolk Care Collaborative performing provider system (“Suffolk PPS”), recognizes that disclosing information on social media can have serious consequences. It is the intention that all individuals and entities that participate in or do business with Suffolk PPS, including but not limited to executives and governing board members, vendors, consultants, contractors of Suffolk PPS, and Coalition Partners working on behalf of Suffolk PPS (PPS Associates) comply with all laws applicable to the Delivery System Reform Incentive Payment (“DSRIP”) Program and Suffolk PPS’ operations, including privacy laws, and accordingly, an appropriate social media policy is consistent with this philosophy.

PROCEDURES:

1. **Privacy/Confidentiality.** Patient privacy and confidentiality must be protected at all times, especially on social media and social networking websites. These sites have the potential to be viewed by many people and any breaches in confidentiality could be harmful to patients and in violation of federal privacy laws, such as HIPAA. PPS Associates have an obligation to prevent unauthorized access to, or use of, patient and personal data and to assure that “de-identified” data cannot be linked back to the patient. Identifiers such as a patient’s name, room number, code name, or pictures should never be used. If disclosed, such an occurrence may constitute a serious HIPAA violation.

2. **Integrity.** Information contained on websites should be truthful and not misleading or deceptive. It should be accurate and concise, up-to-date, and easy for patients to understand. PPS Associates using medical websites should strive to ensure that information provided is, whenever possible, supported by current medical peer-reviewed literature, emanates from a recognized body of scientific and clinical knowledge and conforms to minimal standards of care. It should clearly indicate whether it is based upon scientific studies, expert consensus, professional experience or personal opinion. PPS Associates should avoid requests for online medical advice because it is difficult to verify that the person on the other end of the electronic medium is truly the patient. Furthermore, PPS Associates should also refrain from portraying any unprofessional depictions of themselves on social media and social networking websites as this could reflect negatively on the reputation of Suffolk PPS.

3. **Interacting with Patients.** PPS Associates are discouraged from interacting with current or past patients on personal social networking sites such as Facebook. Online interactions with patients should be limited and these interactions should never occur on personal social networking or social media websites. Even seemingly innocuous online interactions with patients and former patients may violate the boundaries of a proper healthcare provider-patient relationship. PPS Associates should be mindful that while advanced technologies may facilitate the healthcare provider-patient relationship, they can also be a distracter which may lessen the quality of the interactions they have with patients. Such distractions should be minimized whenever possible and a professional position, whether online or in person, should never be used to develop personal relationships with patients.
4. **Posting Content.** PPS Associates should be aware that any information posted on a social networking site may be disseminated (whether intended or not) to a larger audience, and may be taken out of context or remain publicly available online in perpetuity. When posting content online, one should always remember that they are representing Suffolk PPS. PPS Associates should act professionally and take caution not to post information that is ambiguous or that could be misconstrued or taken out of context. Suffolk PPS reserves the right to review Internet communications and posts and edit, modify, delete or request/require the content be edited, modified or deleted. PPS Associates assume all risks related to the security, privacy and confidentiality of their posts. When moderating any website, PPS Associates should delete inaccurate information or other’s posts that violate the privacy and confidentiality of patients or that are of an unprofessional nature.

5. **Professionalism.** To use social media and social networking sites professionally, all PPS Associates should strive to adhere to the following general suggestions:
   
a. Use separate personal and professional social networking sites. For example, use a personal rather than professional e-mail address for logging on to social networking websites for personal use. Others who view a professional e-mail attached to an online profile may misinterpret the PPS Associate’s actions as representing the Suffolk PPS. All personal opinions, views and observations should indicate that they do not reflect the opinions, views and observations of Suffolk PPS.

b. Report any unprofessional and/or disrespectful behavior that is witnessed to supervisory and/or regulatory authorities of Suffolk PPS.

c. Always adhere to the same principles of professionalism online as applicable offline.

d. Cyber-bullying towards any individual is inappropriate and unprofessional.

e. Use discretion in determining the content of posts because the appearance of unprofessionalism may lead patients to question a provider’s competency.

6. **Disclosure.** PPS Associates have an obligation to disclose clearly any information (e.g., financial, professional or personal) that could influence patients’ understanding or use of the information, products or services offered on any website offering health care services or information. PPS Associates must be forthcoming about employment, credentials and conflicts of interest.

7. PPS Associates who have questions about the application of the Social Media Policy to past, present, or future conduct should contact Suffolk PPS’ Information Privacy and Security Officer, who will, in turn, consult with SCC Legal Counsel, as necessary.

8. This Policy is reviewed at least annually by Suffolk PPS’ Information Privacy and Security Officer, or a designee. This policy may be amended from time to time at Suffolk PPS’ discretion.

9. Violations of this Social Media Use Policy by any PPS Associates may result in immediate termination of employment, termination of a contractual relationship with Suffolk PPS, or exclusion from Suffolk PPS.

10. **Coalition Partners.** Each Coalition Partner is responsible for implementing such policies and procedures internally. Each Coalition Partner is independently responsible for ensuring that its internal employees, independent contractors, executives and governing body members are aware of and comply
with such policies and procedures. Each Coalition Partner is responsible for implementing this Policy internally.
BUSINESS ASSOCIATE SUBCONTRACTOR AGREEMENT

This BUSINESS ASSOCIATE SUBCONTRACTOR AGREEMENT, (this “Agreement”), is made by and between SB Clinical Network IPA, LLC d/b/a Suffolk Care Collaborative (“Business Associate”), a limited liability company organized and existing under the laws of the State of New York, and ____________________________ (“Subcontractor”). Business Associate and Subcontractor, collectively, may hereinafter be referred to as the “Parties,” as in the parties to this Agreement. Certain terms used in this Agreement are defined in Section 6.

Preliminary Statement

A. Business Associate has agreed to provide services on behalf of Covered Entities participating as coalition partners of Business Associate’s performing provider system under the New York Delivery System Reform Incentive Payment Program (the “DSRIP Program”). In connection therewith, Business Associate will have access to and/or create PHI and other Personal Information on behalf of the Covered Entities, subject, among other things, to the terms of a HIPAA business associate agreement between Business Associate and the Covered Entity the “Covered Entity Business Associate Agreement”).

B. Pursuant to one or more separate agreements entered into between Business Associate and Subcontractor (the “Subcontracting Arrangement”), Business Associate has engaged Subcontractor to provide services on behalf of Business Associate in connection with the services Business Associate furnishes to the Covered Entities.

C. In connection with the Subcontracting Arrangement, Subcontractor will have access to, use, disclose, create, transmit and/or receive certain PHI and other Personal Information of the Covered Entities in conjunction with the services being provided by Subcontractor to Business Associate, and, on behalf of Business Associate, to the Covered Entities, thus, among other things, necessitating a written agreement between Subcontractor and Business Associate that meets the applicable requirements of HIPAA. The Parties have mutually agreed to satisfy the foregoing regulatory requirements through this Agreement.

D. The Parties are committed to complying with the Health Insurance Portability and Accountability Act of 1996 and all regulations promulgated thereunder, each as amended from time to time, including, without limitation, the Standards for Privacy of Individually Identifiable Health Information (the “Privacy Rule”), the Standards for Security of Electronic Protected Health Information (the “Security Rule”), and the Standards for Notification in the Case of Breach of Unsecured Protected Health Information (the “Breach Notification Rule”) (each such rule at 45 C.F.R. Part 160 and Part 164) (collectively “HIPAA”), as well as with Personal Information Laws. This Agreement, in conjunction with HIPAA and Personal Information Laws, sets forth the terms and conditions pursuant to which PHI (electronic and non-electronic) and other Personal
Information that is created, received, maintained, or transmitted by, Subcontractor from or on behalf of Business Associate, will be handled between Subcontractor and Business Associate and with third parties during the term of their Subcontracting Arrangement and after its termination.

NOW THEREFORE, in consideration of the foregoing and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties hereby agree as follows:

1. **PERMITTED USES AND DISCLOSURES OF PHI.**

   1.1 **Services.** Pursuant to the Subcontracting Arrangement, Subcontractor provides services (“Services”) for Business Associate and, on behalf of Business Associate, to the Covered Entities, that involve the use and disclosure of PHI. Except as otherwise specified herein or in the Subcontracting Arrangement, Subcontractor may make any and all uses of PHI necessary to perform its obligations under the Subcontracting Arrangement. All other uses not authorized by this Agreement or required by applicable law are prohibited. Moreover, Subcontractor may disclose PHI for the purposes authorized by this Agreement, and only: (a) to its employees, subcontractors and agents, in accordance with Section 2.1(d) of this Agreement; and (b) as otherwise permitted by or as required by HIPAA.

   1.2 **Business Activities of the Subcontractor.** Unless otherwise limited herein, Subcontractor may not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by the Covered Entity, except that Subcontractor may:

      (a) use PHI for the proper management and administration of Subcontractor, or to carry out the legal responsibilities of Subcontractor, provided that such uses are permitted under applicable laws;

      (b) disclose PHI for the proper management and administration of Subcontractor, or to carry out the legal responsibilities of Subcontractor, provided that Subcontractor represents to Business Associate, in writing, that the disclosures are Required by Law, or Business Associate obtains written assurances from the person to whom the information is disclosed that the information will remain confidential and be used or further disclosed only as Required by Law or for the purposes for which it was disclosed to the person, and notifies the Subcontractor of any instances of which it is aware in which the confidentiality of the information has been breached; and

      (c) provide Data Aggregation services on behalf of Business Associate, relating to the Health Care Operations of the Covered Entity.

2. **RESPONSIBILITIES OF SUBCONTRACTOR.**

   2.1 **Responsibilities of Subcontractor.** Subcontractor hereby agrees to do the following:

      (a) Not use or disclose PHI other than as permitted or required by this Agreement or as Required by Law.

      (b) Use appropriate administrative, technical and physical safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to Electronic PHI, to prevent use or disclosure of PHI other than as provided for by the Agreement.
(c) Notify Business Associate, in writing, within five (5) business days of becoming aware of (i) any use or disclosure of Protected Health Information or Personal Information by Subcontractor or any of its agents or subcontractors, that is contrary to this Agreement, which shall be deemed to include, without limitation, any Breach of Unsecured Protected Health Information, and any Personal Information Law Breach; or (ii) any Security Incident. If there is such Breach of Unsecured Protected Health Information or a Personal Information Law Breach, Subcontractor will:

(i) Notify Business Associate in writing of the Breach or Personal Information Law Breach without unreasonable delay, and in no event more than five (5) business days after discovery of the Breach or Personal Information Law Breach, and provide: (A) with respect to the Breach, to the extent possible: (i) the identification of all Individuals affected by the Breach, and (ii) any other available information that the Covered Entity is required to include in notifications to such Individuals pursuant to 45 C.F.R. § 164.404(c); and (B) with respect to the Personal Information Law Breach, all of the elements specified in any applicable Personal Information Laws, including, without limitation, all information necessary for the Covered Entity or Business Associate to provide any applicable notice required to be provided by the Covered Entity or Business Associate under any applicable Personal Information Laws. In the event any such information is not available when Business Associate is notified of the Breach and/or Personal Information Law Breach, Subcontractor will provide such information to Business Associate as soon as it becomes available;

(ii) Cooperate with Business Associate to notify, at Subcontractor’s expense: (A) in the manner and within the time periods specified for the Covered Entity in the Breach Notification Rule (I) Individuals whose Unsecured Protected Health Information has been, or is reasonably believed by Subcontractor to have been, accessed, acquired, used, or disclosed, (II) the media, as required pursuant to 45 C.F.R. § 164.406, and (III) the Secretary, as required by 45 C.F.R. § 164.408; and (B) in the manner and within the time periods specified for the Covered Entity and/or Business Associate in Personal Information Laws, such persons required to be notified pursuant to Personal Information Laws. Subcontractor shall, upon Company’s written direction, directly provide the notifications set forth in this Section 2.1(c)(ii) on behalf of the Covered Entity and/or Business Associate. Subcontractor will not initiate any of the notifications set forth in this Section 2.1(c)(ii) without Business Associate’s written approval; and

(iii) Be responsible for all costs involved in fulfilling the notification requirements set forth in this Section 2.1(c) and otherwise applicable to Subcontractor, Business Associate, or the Covered Entity in connection with the Breach Notification Rule and Personal Information Laws, if resulting from a Breach or Personal Information Law Breach by Subcontractor or its agents or subcontractors, whether such costs are incurred initially by Subcontractor, Subcontractor’s agents or subcontractors, or by the Covered Entity or Business Associate.

(d) In accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any agents or subcontractors that create, receive, maintain, or transmit PHI on behalf of Subcontractor agree in writing to the same restrictions, conditions, and requirements that apply to Subcontractor under this Agreement with respect to such PHI.

(e) Ensure that Subcontractor, and any agent or subcontractor of Subcontractor, shall not, without the prior written consent of Business Associate, export such PHI or other Personal Information beyond the borders of the United States of America. In this context, an “export” outside the United States of America occurs if Subcontractor’s workforce members, or its agents or subcontractors, physically located outside the United States of America are able to access, use, or disclose PHI or other...
Personal Information. If Subcontractor or its agent or subcontractor desires to export PHI or other Personal Information beyond the borders of the United States of America, then, subject to the United States and New York State export control and foreign outsourcing laws, rules and regulations, Subcontractor will provide to Business Associate prior to such export, a reasonable assurance, evidenced in writing, that Subcontractor and its applicable agent or subcontractor will comply with the privacy and security obligations of Subcontractor set forth either in this Agreement, and with applicable law, rules and regulations, with respect to such PHI and other Personal Information.

(f) Provide Business Associate, upon receipt of Business Associate's written request, a list of all agents and subcontractors that create, receive, maintain, or transmit PHI on behalf of Subcontractor.

(g) Within ten (10) business days of a request from Business Associate or a Covered Entity, make available PHI in a Designated Record Set, if applicable, to Business Associate or Covered Entity, as necessary to satisfy a Covered Entity’s obligations under 45 C.F.R. 164.524, and to satisfy Business Associate’s obligations under the Covered Entity Business Associate Agreement. If an Individual or Covered Entity requests access to PHI directly from Subcontractor, or, to Subcontractor’s knowledge, its agents or subcontractors, if any, Subcontractor must notify Business Associate, in writing, within five (5) business days of becoming aware of the request.

(h) Within ten (10) business days of receipt of a request from Business Associate or a Covered Entity, make any amendment(s) to PHI, if applicable, in a Designated Record Set, as directed or agreed to by Business Associate or the Covered Entity, pursuant to 45 C.F.R. § 164.526, or take other measures as necessary to satisfy Covered Entity’s obligations under 45 C.F.R. § 164.526 and to satisfy Business Associate’s obligations under the Covered Entity Business Associate Agreement. If an Individual or Covered Entity requests an amendment of PHI directly from Subcontractor, or, to Subcontractor’s knowledge, its agents or subcontractors, if any, Subcontractor must notify Business Associate in writing within five (5) business days of becoming aware of the request.

(i) As applicable, maintain and make available to Business Associate or to a Covered Entity, within ten (10) business days of request by Business Associate or Covered Entity, the information required for the Covered Entity to satisfy the Covered Entity’s obligations pursuant to 45 C.F.R. § 164.528 and to satisfy Business Associate’s obligations under the Covered Entity Business Associate Agreement, to respond to a request for an accounting of disclosures of PHI. If an Individual or Covered Entity requests an accounting of disclosures of PHI directly from Subcontractor or, to Subcontractor’s knowledge, its agents or subcontractors, if any, Subcontractor must notify Business Associate in writing within five (5) business days of becoming aware of the request.

(j) To the extent Subcontractor is to carry out one or more of a Covered Entity’s obligation(s) under Subpart E of 45 C.F.R. Part 164, comply with the requirements of Subpart E that apply to Covered Entity in the performance of such obligation(s).

(k) Upon request, make its internal practices, books, and records: (i) available to the Secretary for purposes of determining compliance with HIPAA, and (ii) to Business Associate for purposes of determining compliance with this Agreement. Subcontractor shall notify Business Associate within three (3) business days of receiving any such request from the Secretary.

(l) Comply with minimum necessary requirements under HIPAA.
2.2 **Electronic Data Interchange.** Subcontractor agrees, in connection with all services that it provides on behalf of Business Associate, to satisfy all applicable provisions of the HIPAA standards for electronic transactions and code sets, also known as the “Electronic Data Interchange (‘EDI’) Standards,” including at 45 C.F.R. Part 162. Subcontractor further agrees to ensure that any of its agents or subcontractor that conducts standard transactions, as such term is defined at 45 C.F.R. §162.103, on its behalf will comply with the EDI Standards in connection with all services provided on behalf of Business Associate.

2.3 **Certain DEAA Requirements.**

(a) With respect to any MCD/PHI made available to Subcontractor in connection with this Agreement, Subcontractor acknowledges and agrees that it is deemed to be a third party subcontractor of SBUH under the DEAA, and that SBUH is required to include certain provisions in any subcontract with any such third party contractor who will have access to such MCD/PHI. Accordingly, with respect to any MCD/PHI, Subcontractor agrees to comply with all DOH requirements for the release of such data to Subcontractor, which may include, without limitation, implementing administrative, physical and technical safeguards as required by the DOH, including but not limited to two factor authorization for access and data encryption. As used herein: “two factor authentication” is understood to be a security process in which the user provides two means of identification using at a minimum two of the following: something the user knows (knowledge factor – pin, username, password), something the user has (possession factor – hard or soft token), and/or something the user is (inherence factor – biometric); and “encryption” is understood to be the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

(b) Subcontractor, in accordance with the requirements of the DEAA, and with respect to any MCD/PHI agrees to comply with the following state and federal laws and regulations:

i. Section 367b(4) of the NY Social Services Law

ii. New York State Social Services Law Section 369 (4)

iii. Article 27-F of the New York Public Health Law & 18 NYCRR 360-8.1

iv. Social Security Act, 42 USC 1396a (a)(7)


vi. HIPAA

(c) In accordance with the requirements of the DEAA, notice is hereby given that MCD/PHI and other Personal Information released to Subcontractor may contain AIDS/HIV related confidential information as defined in Section 2780(7) of the New York Public Health Law. As required by New York Public Health Law Section 2782(5), the following notice is provided to Subcontractor:

“This information has been disclosed to you from confidential records which are protected by state law. State law prohibits you from making any further disclosure of this information without the specific written consent of the person to whom it pertains, or as otherwise permitted by law. Any unauthorized further disclosure in violation of
state law may result in a fine or jail sentence or both. A general authorization for the release of medical or other information is NOT sufficient authorization for the release for further disclosure.”

In addition, Subcontractor hereby acknowledges and agrees that Business Associate has otherwise notified Subcontractor that Subcontractor is required to comply with the confidentiality, disclosure and re-disclosure requirements of 10 NYCRR Part 63 to the extent such requirements may be applicable.

(d) **Notice Regarding Alcohol and Substance Abuse Related Confidentiality Restrictions.** Alcohol and substance abuse information is confidential pursuant to 42 C.F.R. Part 2. General authorizations are ineffective to obtain the release of such data. The federal regulations provide for a specific release for such data.

(e) **MCD PHI Requirement.** Subcontractor agrees to the same restrictions and conditions that apply throughout the DEAA. Subcontractor shall not further disclose the MCD PHI without the prior written approval of the New York State Department of Health.

(f) **Notices.** Subcontractor agrees to include the notices preceding (in this Section 2.3), as well as references to statutory and regulatory citations set forth above, in any agreement, contract or document that Subcontractor enters into that involves MCD PHI.

3. **RESPONSIBILITIES OF BUSINESS ASSOCIATE.**

3.1 With regard to the use and/or disclosure of PHI by Subcontractor, Business Associate hereby agrees:

(a) to inform Subcontractor of any limitations in the Notice of Privacy Practices that a Covered Entity provides to individuals pursuant to 45 C.F.R. §164.520, of which Business Associate is aware, to the extent that such limitation may affect Subcontractor’s use or disclosure of PHI hereunder.

(b) to inform Subcontractor of any changes in, or revocation of, the permission by an Individual to use or disclose PHI, of which Business Associate is aware, to the extent that such limitation may affect Subcontractor’s use or disclosure of PHI hereunder.

(c) to notify Subcontractor of any restriction on the use or disclosure of PHI that a Covered Entity has agreed to or is required to abide by under 45 C.F.R. 164.522, of which Business Associate is aware, to the extent that such restriction may affect Subcontractor’s use or disclosure of PHI.

4. **TERM AND TERMINATION.**

4.1 **Term.** The Term of this Agreement shall commence on the date of the last signature below and shall terminate on the termination date of the Subcontracting Agreement or on the date Business Associate terminates this Agreement for cause as authorized in paragraph 4.2 of this Section, whichever is sooner.

4.2 **Termination for Cause.** If Business Associate determines Subcontractor has violated
a material term of the Agreement and Subcontractor has not cured the breach or ended the violation within the time specified by Business Associate, Business Associate may terminate this Agreement.

4.3 **Obligations of Subcontractor upon Termination.** Upon termination of this Agreement for any reason, Subcontractor will, and will ensure that its agents and subcontractors that have had access to PHI and other Personal Information will:

i. Retain only the PHI and other Personal Information that is necessary for Subcontractor or Subcontractor’s agents and subcontractors, to continue its proper management and administration or to carry out its legal responsibilities, and return to Business Associate or to Business Associate’s designee, or upon Business Associate’s prior written agreement, destroy (and certify in writing to the Business Associate that it has destroyed) any remaining PHI or other Personal Information that Subcontractor or its agents or subcontractors maintain in any form;

ii. Continue to use appropriate administrative, technical and physical safeguards, and to comply with Subpart C of 45 C.F.R. Part 164, with respect to any Electronic Protected Health Information or other Personal Information, so as to prevent use or disclosure of the Electronic Protected Health Information and other Personal Information other than as specified in this Section 4.3, for as long as Subcontractor or any Subcontractor agent or subcontractor retains the Electronic Protected Health Information or other Personal Information;

iii. Not use or disclose the PHI or other Personal Information retained by Subcontractor or by any Subcontractor agent or subcontractor, other than for the purposes for which such PHI or other Personal Information was retained, and subject to all the conditions and limitations set forth in Sections 1 and 2 above that applied prior to termination of the Agreement;

iv. Return to Business Associate or, upon Business Associate’s prior written agreement, destroy (and certify in writing to Business Associate that it has destroyed) the PHI and other Personal Information retained by Subcontractor or by any Subcontractor agent or subcontractor, as of the date such PHI or other Personal Information is not needed by Subcontractor or any Subcontractor agent or subcontractor for its proper management and administration or to carry out its legal responsibilities.

If it is not feasible for Subcontractor to return or destroy any PHI or other Personal Information, Subcontractor will notify Business Associate in writing and Business Associate may disagree with Subcontractor’s determination. Said notification shall include: (a) a statement that Subcontractor has determined that it is not feasible to return or destroy the PHI or other Personal Information in its possession, and (b) the specific reasons for such determination. Subcontractor further agrees to extend any and all protections, limitations and restrictions contained in this Agreement to Subcontractor’s use and/or disclosure of any PHI or other Personal Information retained after the termination of this Agreement, and to limit any further uses and/or disclosures to the purposes that make the return or destruction of the PHI infeasible, including when applicable those under Sections 1 and 2 of this Agreement. If it is infeasible for Subcontractor to obtain from a subcontractor or agent any PHI or other Personal Information in the possession of the subcontractor or agent, Subcontractor must provide a written explanation to Business Associate and require such
subcontractor or agent to agree to extend any and all protections, limitations and restrictions contained in this Agreement to the subcontractor’s and/or agent’s use and/or disclosure of any PHI or other Personal Information retained after the termination of this Agreement, and to limit any further uses and/or disclosures to the purposes that make the return or destruction of the PHI or other Personal Information infeasible.

Subcontractor’s obligations under this Section 4.3 shall survive the expiration or termination of this Agreement for any reason.

4.4 Automatic Termination. This Agreement will automatically terminate without any further action of the Parties upon the termination or expiration of the Subcontracting Arrangement.

5. MISCELLANEOUS.

5.1 Amendments; Waiver. This Agreement may not be modified, nor shall any provision hereof be waived or amended, except in a writing duly signed by authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of HIPAA and any other applicable law.

5.2 Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with HIPAA.

5.3 No Third Party Beneficiaries. Nothing expressed or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the Parties and the respective successors or assigns of the Parties, any rights, remedies, obligations, or liabilities whatsoever.

5.4 Notices. Whenever, under the terms of this Agreement, written notice is required or permitted to be given by a Party to the other Party, such notice shall be deemed to have been sufficiently given if given: (A) by hand delivery, (B) by U.S. Postal Service certified mail, return receipt requested, postage prepaid, (C) by nationally recognized overnight express delivery service, charges prepaid, in each case addressed to the Party to whom it is to be given, at such Party’s address given on the signature page hereof, and/or (D) (other than for the delivery of fees) via facsimile or email to the facsimile telephone numbers or email addresses listed below. A copy of any such notice shall also be given in the same manner to the Party’s Privacy Officer, if any, listed on the signature page hereof. Either Party hereto may change its respective address by written notice in accordance with this paragraph. Notice is deemed given when received at the applicable address, as indicated by proof of delivery.

5.5 Disputes. If any controversy, dispute or claim arises between the Parties with respect to this Agreement, the Parties shall make good faith efforts to resolve such matters informally.

5.6 Changes in Law. The Parties recognize that this Agreement is at all times subject to applicable state, local, and federal laws. The Parties further recognize that this Agreement may become subject to amendments in such laws and regulations and to new legislation. Any provisions of law that invalidate, or are otherwise inconsistent with, the material terms and conditions of this Agreement, or that would cause one or both of the Parties hereto to be in violation of law, shall be deemed to have superseded the terms of this Agreement and, in such event, the Parties agree to use their best efforts to modify in an executed written agreement the terms and conditions of this Agreement to be consistent with the
requirements of such law(s) in order to effectuate the purposes and intent of this Agreement within thirty (30) days of receipt of notice from one Party to the other Party setting forth the proposed changes.

5.7 **Construction of Terms.** The terms of this Agreement shall be construed in light of any applicable interpretation or guidance on HIPAA issued by the Department of Health and Human Services of the Office of Civil Rights, and any successor agency, from time to time.

5.8 **Governing Law.** This Agreement shall be governed by New York law notwithstanding any conflicts of law provisions to the contrary.

5.9 **Indemnification.** Subcontractor will, during and after the term of this Agreement, hold Business Associate, and its respective officers, directors, employees, agents and affiliates, harmless from, and defend and indemnify each of them against, any and all claims, losses, liabilities, penalties, fines, costs, damages and expenses, including, without limitation, reasonable attorneys’ fees and costs, incurred by, imposed upon or asserted against any of them as a result, directly or indirectly, of Subcontractor’s or any of its agents or subcontractors’ directors’, officers’, employees’ or agents’ breach of this Agreement, HIPAA, the Privacy Rule, the Security Rule, the Breach Notification Rule or Personal Information Laws.

5.10 **Independent Contractors.** Nothing contained herein shall be deemed or construed by the Parties or by any third party, to create a relationship of employer and employee, principal and agent, or joint venture between Subcontractor and Business Associate, it being understood and agreed that Subcontractor provides services to Business Associate hereunder as an independent contractor, and that without in any manner limiting the obligations of Subcontractor under this Agreement and the Subcontracting Arrangement, Subcontractor retains full control and discretion over its performance under this Agreement and the Subcontracting Arrangement, and Business Associate has no authority to direct or control Subcontractor’s conduct in the course of performing this Agreement and the Subcontracting Arrangement.

5.11 **Further Assurances.** The Parties agree to execute and deliver, or cause to be executed and delivered, such further instruments or documents as the Parties mutually agree are necessary to carry out the intentions of the Parties as set forth in this Agreement.

5.12 **Counterparts.** This Agreement may be executed in any number of counterparts, each of which shall be deemed an original.

6. **DEFINITIONS.**

6.1 **Generally.** The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure (whether or not capitalized, as the context requires, and all derivatives thereof), Health Care Operations, Individual, Notice of Privacy Practices, Secretary, Security Incident, Unsecured Protected Health Information, and Use (whether or not capitalized, as the context requires, and all derivatives thereof).

6.2 **Specific Definitions.** Specific definitions include:

(a) **Business Associate.** “Business Associate” shall generally have the same meaning as the term “business associate” at 45 C.F.R. 160.103, and in reference to the party to this Agreement, shall mean the Party identified as the Business Associate above.
(b) Covered Entity. “Covered Entity” shall generally have the same meaning as the term “Covered Entity” at 45 C.F.R. 160.103, and in reference to the party to this Agreement, shall mean the coalition partners of Business Associate under the DSRIP Program who are Covered Entities for purposes of HIPAA.

(c) DEAA. “DEAA” shall mean that certain Data Exchange Application and Agreement between SBUH and DOH.

(d) DOH. “DOH” shall mean the New York State Department of Health.

(e) Electronic Protected Health Information or Electronic PHI. “Electronic PHI” shall mean PHI which is transmitted by Electronic Media (as defined in HIPAA) or maintained in Electronic Media.

(f) MCD/PHI. “MCD/PHI” shall mean “Medicaid Confidential Data/Protected Health Information” as defined in this Agreement.

(g) Medicaid Confidential Data/Protected Health Information. “Medicaid Confidential Data/Protected Health Information” shall mean all information about a recipient or applicant, including enrollment information, eligibility data and protected health information, which is originated from DOH under the DEAA and received by Subcontractor, except limited to the information received from Business Associate, or created, received or maintained on behalf of Business Associate.

(h) Personal Information. “Personal Information” shall mean individually-identifying information received from Business Associate, or created, received or maintained on behalf of Business Associate, the confidentiality, privacy and/or security of which is protected under applicable laws other than, or in addition to, HIPAA.

(i) Personal Information Laws. “Personal Information Laws” shall mean applicable laws, other than HIPAA, that concern the confidentiality, privacy and/or security of Personal Information.

(j) Personal Information Law Breach. “Personal Information Law Breach” shall mean any use or disclosure of Personal Information that would require data breach notification to Participants, the media, and/or government agencies or officials by Business Associate, and/or Company, under applicable Personal Information Laws.

(k) PHI. “PHI” shall mean “Protected Health Information,” as defined in this Agreement.

(l) Privacy Officer. “Privacy Officer” shall have the meaning as set out in its definition at 45 C.F.R. § 164.530(a)(l) as such provision is currently drafted and as it is subsequently updated, amended or revised, and in reference to this Agreement, shall mean the person identified as the Privacy Officer above.

(m) Protected Health Information. “Protected Health Information” shall have the meaning given to the term Protected Health Information in 45 C.F.R. § 160.103, except limited to the information received from Business Associate, or created, received or maintained on behalf of Business Associate. For the purposes of this Agreement, “Protected Health Information” and “PHI” shall also
include any New York State Medicaid Confidential Data/Protected Health Information ("MCD/PHI").

(n) **Required by Law.** "Required by Law" shall have the meaning given to the term under the Privacy Rule including, but not limited to, 45 C.F.R. 164.103, and any additional requirements created under HITECH.

(o) **SBUH.** "SBUH" shall mean the State University of New York at Stony Brook University Hospital.

[Remainder of page intentionally left blank; signature page follows]
IN WITNESS WHEREOF, each Party hereto has caused this Business Associate Subcontractor Agreement to be duly executed in its name and on its behalf, on the dates set forth below.

BUSINESS ASSOCIATE:

____________________________________
By: ____________________________
Name: ____________________________
Title: ____________________________
Date: ____________________________

SUBCONTRACTOR:

____________________________________
By: ____________________________
Name: ____________________________
Title: ____________________________
Date: ____________________________

Facsimile: ____________________________
Email: ____________________________
Privacy Officer: ____________________________

Facsimile: ____________________________
Email: ____________________________
Privacy Officer: ____________________________
SUFFOLK CARE COLLABORATIVE

BREACH NOTIFICATION POLICY

PURPOSE: SB Clinical Network IPA, LLC, doing business as Suffolk Care Collaborative performing provider system (the “Suffolk PPS”), is required to notify affected individuals and applicable government agencies, as soon as possible, but in no event more than 60 days after the date of discovery of a breach of unsecured protected health information in accordance with the requirements of the HITECH Act and the New York State Office of Information Technology Service Breach Notification Law.

DEFINITIONS:

**Breach** means the acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA privacy regulations which compromises the security or privacy of PHI.\(^1\) An acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA privacy regulations is presumed to be a Breach unless it is demonstrated that there is a low probability that the PHI has been compromised based on a risk assessment. The Chief Information Privacy and Security Officer in collaboration with SCC leadership determines the probability of a breach.

**Disclosure** means the release, transfer, provision of access to, or divulging in any other manner of PHI outside Suffolk PPS.

**Use** means the sharing, employment, application, utilization, examination, or analysis of such information within Suffolk PPS.

**DHHS** means the U.S. Department of Health and Human Services.

**HIPAA** means the federal Health Insurance Portability and Accountability Act of 1996 (42 USC § 201 et seq) and its implementing regulations (45 CFR Part 160 and Part 164).

**HITECH Act** means the federal Health Information Technology for Economic and Clinical Health Act and its implementing regulations (including 45 CFR 164.400-164.414).

**Protected Health Information** (“PHI”) is information that:

- A. Is created by a health plan, health care provider, health care clearinghouse or an employer;
- B. Relates to an individual’s physical or mental health, the provision of health care to an individual, or the payment for the provision of health care to an individual; and

\(^1\) Note: A Breach does not require notice under the HITECH Act if it involves PHI de-identified in accordance with HIPAA standards or limited data sets when dates of birth and zip codes have been removed.
C. Identifies, or could be reasonably expected to be used to identify, an individual.

Unsecured Protected Health Information (“Unsecured PHI”) means PHI or electronic PHI (e-PHI) that has not been rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of DHHS.

PROCEDURES:

1. DISCOVERY OF BREACH

   a. Reporting Breaches. All affected employees and persons associated with the Suffolk PPS, including executives and governing body members (“PPS Affiliates”) must immediately inform Suffolk PPS’s Chief Information Privacy and Security Officer of any potential Breach as soon as possible. While investigating any potential Breach, the Chief Information Privacy and Security Officer documents the incident using the “Report Form” refer to Exhibit C. Subcontractor business associates of Suffolk PPS report all potential Breaches in accordance with their subcontractor business associate agreements.

   All Coalition Partners in Suffolk PPS are responsible for reporting any potential Breach involving PHI/e-PHI relating to the Delivery System Reform Incentive Program immediately to Suffolk PPS’ Chief Information Privacy and Security Officer. Suffolk PPS coordinates directly with the Coalition Partner in order to oversee the investigation and any notification requirements, as necessary.

   b. Date of Discovery. A Breach is considered to have occurred at the time of the impermissible access, use or disclosure of Unsecured PHI. A Breach is not, however, considered to have been discovered, for the purposes of the HITECH Act, until:

      i. the first day the Breach is known to the Suffolk PPS or PPS Affiliate; or

      ii. the first day that Suffolk PPS or PPS Affiliate, by exercising reasonable diligence, should have known of the Breach.

2. INVESTIGATION

   a. Conduct an Investigation. After receiving a report of a potential Breach, the Information Privacy and Security Officer promptly investigates the circumstances surrounding the potential Breach with other Suffolk PPS representatives as necessary to conduct such investigation. During the investigation, the Chief Information Privacy and Security Officer, to the extent possible:

      i. determine whether there has been an impermissible access, use or disclosure of PHI;

      ii. determine who impermissibly accessed, used or received PHI and to whom the PHI was potentially disclosed, if applicable;

      iii. determine whether the PHI involved in the incident was Unsecured PHI (e.g., was it encrypted);

      iv. identify the type and amount of PHI involved; and
v. determine what steps have been taken (or should be taken) to mitigate risk (e.g., a confidentiality agreement with the person who received the PHI, obtaining the return of the PHI, reporting the incident to the police, etc.).

b. **Notification Prior to the Conclusion of the Investigation.** In some situations in which it is apparent that a Breach has occurred, initial individual notifications may need to be sent prior to the completion of the investigation. The Information Privacy and Security Officer is responsible for making a determination of the appropriate timing of the notification based on the requirements of the HITECH Act (See Section III(c)(3) below).

3. **DETERMINATION IF A BREACH OCCURRED**

   a. **Breach Determination.** Whenever a potential Breach is reported, it is presumed that a Breach has occurred, unless it is demonstrated that there is a low probability that the PHI has been compromised. In addition, the state requirements noted in Exhibit A is reviewed.

   b. **Notification.** If it is determined that a Breach has occurred, individuals are notified as described in Section 3 (d); or

   c. **Risk Assessment.** If it is determined that a Breach has not occurred because an exception applies or it is determined that there is a low probability that the PHI has been compromised, the Chief Information Privacy and Security Officer documents a risk assessment which supports the conclusion that notification of individuals was not required. In making such determination, the Chief Information Privacy and Security Officer considers the factors listed on the “Risk Assessment” form Exhibit B.

   d. **Exceptions.** The following do not constitute a Breach and therefore notification to individuals under the HITECH Act is not required:

      i. The unintentional acquisition, access, or use of PHI by a PPS Affiliate, or another individual acting under a covered entity’s or a business associate’s authority if the acquisition, access, or use was made in good faith, within the scope of such individual’s authority, and does not result in further unauthorized use or disclosure.

      ii. The inadvertent disclosure of PHI from one person to another person, if both persons were authorized to access the PHI at the same covered entity or business associate, so long as the PHI is not further acquired, accessed, used or disclosed in an unauthorized manner.

      iii. The unauthorized disclosure of PHI when the covered entity or business associate has a good faith belief that the person to whom disclosure was made would not reasonably have been able to retain the information.

4. **NOTIFICATION OF AFFECTED INDIVIDUALS**

   a. **Time Frame for Notification.** If it is determined that notification is required, such notification is made without unreasonable delay, but in no event more than 60 days from the Date of Discovery of the Breach. Suffolk PPS may delay Breach notifications if a delay is requested by a law enforcement official:
i. If the request is in writing on official letterhead, the delay may be for as long as requested.

ii. If it is an oral request, the delay may be for up to 30 days unless a further delay is requested in writing on official letterhead. All oral requests are documented by Suffolk PPS or Chief Chief Information Privacy and Security Officer including the date/time and name of the official making the request.

b. **Content of the Notification.** The Chief Information Privacy and Security Officer is responsible for arranging the preparation of the required notices of Breaches to individuals. Such notifications must be written in plain language, at an appropriate reading level, using clear language and syntax and must include the following information:

   i. A brief description of what happened, including the date of the Breach and Date of Discovery of the Breach, if known;

   ii. A description of the types of Unsecured PHI involved in the Breach;

   iii. Any steps individuals may wish to take to protect themselves from potential harm resulting from the Breach;

   iv. A brief description of Suffolk PPS’s efforts to investigate the Breach, mitigate harm to individuals, and protect against further Breaches; and

   v. Contact information for individuals to ask questions or learn information about the Breach, to include a toll-free telephone number, an email address, a website and postal address.

   **Note:** Notices do not include a specific list of the actual PHI that was breached or other sensitive information, just a general description of the type(s) of PHI involved in the Breach.

c. **General Method of Notification.** Notice to the individuals affected by a Breach is provided in written form by first-class mail at the last known address of the individual. Written notice may be provided by e-mail only if the individual agrees to receive e-mail notice and has not withdrawn such agreement.

   i. Notice to a minor or an individual who otherwise lacks legal capacity due to a physical or mental condition is made to the parent or personal representative of the individual.

   ii. If Suffolk PPS knows that the individual is deceased and has the address of next of kin or the individual’s personal representative, notice is sent to the next of kin or personal representative, and not to the individual’s emergency contact unless the individual’s emergency contact is the individual’s next of kin or personal representative. Suffolk PPS is not required to provide substitute notice to next of kin or a personal representative if Suffolk PPS does not have contact information or has out-of-date contact information for the next of kin or personal representative.
Note: Urgent Notice may be made when the Chief Information Privacy and Security Officer determines that there is a possibility of imminent misuse of Unsecured PHI. The Chief Information Privacy and Security Officer, in these cases, may notify affected individuals by telephone, e-mail or other means, as well as by written notice.

d. Substitute Notice. Substitute notice to the individuals is provided if Suffolk PPS has insufficient or out-of-date contact information for affected individuals.

i. If there are fewer than 10 individuals for whom Suffolk PPS has insufficient or out-of-date contact information, an alternative form of notice, such as by telephone or e-mail, newspaper or website is used.

ii. If there are 10 or more individuals for whom Suffolk PPS has insufficient or out-of-date contact information, Suffolk PPS provides the following forms of substitute notice:

1. Either (A) conspicuous posting for a period of 90 days on the website homepage or by a noticeable and obvious hyperlink to the information; or (B) conspicuous notice in major print or broadcast media in geographic areas where the affected individuals are likely to reside; and

2. A toll-free phone number, active for 90 days, at which individuals can learn whether their Unsecured PHI was included in the Breach.

5. NOTIFICATIONS TO AUTHORITIES

a. Annual Notification to Secretary. The Chief Information Privacy and Security Officer maintains documentation of Breaches involving less than 500 individuals. The “Report Form” Exhibit C can be used for this purpose. The Chief Information Privacy and Security Officer submits to the Secretary, on an annual basis, information regarding Breaches that occurred during the preceding year. Suffolk PPS submits this information no later than 60 days after the end of each calendar year in which the Breach is discovered. The information included in the Breach log includes all of the information included in the Breach notices to individuals.

b. Notification to DHHS and the Media When 500 or More Affected Individuals are Involved. When the Breach involves 500 or more individuals of a state, notice must be given to the Secretary of DHHS at the same time that notices are given to individuals. Notice must also be provided to prominent media outlets in the state through a press release.

i. Notification to the media must include the same information included in written notices to individuals.

ii. Notification to the media is made without unreasonable delay, and in no case later than 60 calendar days following the Date of Discovery of the Breach.

6. MITIGATION. Suffolk PPS takes reasonable efforts to mitigate the effects of a Breach and to reduce harm to individuals in accordance with its privacy and security policies which may include but is not limited to the following: providing credit monitoring services to individuals, retraining
staff on privacy policies, or implementing new technical or physical safeguards to protect the privacy of PHI.

7. **ADDITIONAL REQUIREMENTS**

   a. **Security Incident.** To the extent that a Breach involves a security incident, the Suffolk PPS Chief Information Privacy and Security Officer follows the guidelines in the Suffolk PPS’ policy regarding responses to security incidents.

   b. **Sanctions.** If sanctions against a PPS Affiliate result from a Breach, Suffolk PPS’ policy regarding sanctions/disciplinary actions are followed, including, as appropriate, a notation on Suffolk PPS’s HIPAA sanctions log.

8. **Policy Review:** This policy is reviewed at least annually by the Suffolk PPS’s Chief Information Privacy and Security Officer, or designee. This policy may be amended from time to time at the Suffolk PPS’s discretion.

9. **COALITION PARTNERS.** Each Coalition Partner is responsible for implementing such policies and procedures internally. The Coalition Partner is independently responsible for ensuring that its internal employees, independent contractors, executives and governing body members are aware of and comply with such policies and procedures.
Exhibit A

NYS BREACH NOTIFICATION REQUIREMENTS

Additional state notification requirements may be required when individuals’ social security numbers or other financial information is included about state residents.

DEFINITIONS


Private Information means information consisting of an individual’s PHI in combination with any one or more of the following data elements about the individual, when either the applicable information is not encrypted or when it is encrypted and the encryption key has also been compromised:

1. Social security number;
2. Driver’s license number or non-driver identification card number; or
3. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

Private Information does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.

Security Breach means an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of Private Information about New York residents maintained by Suffolk PPS. In determining whether information is reasonably believed to have been acquired by an unauthorized person, Suffolk PPS may consider the following factors, among others:

1. indication that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information;
2. indication that the information has been downloaded or copied; or
3. indication that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

B. NOTIFICATIONS

1. Security Breaches. If the Breach is also a Security Breach, (Private Information such as social security number was involved) and New York residents are affected, Suffolk PPS also notifies the N.Y. Attorney General, the N.Y. Department of State Division of Consumer Protection, and the N.Y. State Office of Cyber Security and Critical Infrastructure. If more than 5,000 New York residents are affected, Suffolk PPS notifies consumer reporting agencies.

2. Notice Contents. Such notices to these state and consumer agencies must include a copy of the notifications sent to affected individuals, a description of when and how the notifications were sent and the approximate number of affected individuals.
EXHIBIT B

RISK ASSESSMENT FORM

Date: _____________________  Name: _____________________

Date of Incident: ________________  Date of Discovery of Incident: ________________

Brief Description of Incident:
__________________________________________________________________________________

I. The nature and extent of the PHI involved, including types of identifiers and likelihood of re-identification.
   A. Describe the patient information involved.
   B. Were direct patient identifiers of information included? (i.e. names or social security numbers of patients) YES or NO
   C. If no direct identifiers of information were provided, is there a likelihood that the PHI involved could be re-identified based on the context and the ability to link the PHI with other available information? YES or NO
   D. Is PHI that was involved sensitive in nature? YES or NO
       If Yes, please describe in further detail below.

II. Unauthorized person who used the PHI or to whom the disclosure was made
   A. Who accessed/used the information or to whom was the information disclosed?
   B. Was the information disclosed to someone with obligations to protect the privacy of the PHI? (e.g. covered entity, attorney) Please explain. YES OR NO
   C. Was the PHI disclosed to someone with a reason to want to misuse the PHI? (e.g. to an employer or family member) Please explain. YES or NO

III. Was the PHI actually acquired or viewed
    Can you demonstrate that PHI was not accessed (i.e. a laptop was stolen but a forensic analysis shows that the PHI was not accessed) Please explain. YES or NO

IV. Extent to which the risk of the PHI has been mitigated
    A. Have you received satisfactory assurances from the person who received the PHI that they destroyed the information and did not share the PHI? Please explain and attach written attestation if available. YES or NO
    B. Describe any other mitigating factors: ________________________________

CONCLUSION (describe why the combination of these factors supports a finding that there was a low probability of compromise):
Exhibit C

Report Form - Potential HIPAA Breaches

Breach Affecting.

_____ 500 or more patients  
_____ Less than 500 patients

If any business associates were involved in the Breach, please provide the following information:

Name of Business Associate: ________________________________

Description of Breach.

Date(s) of Breach: ____________________  
Date(s) of Discovery: ____________________

Approximate Number of Patients Affected by the Breach: ____________________

Type of Breach (Check where appropriate)

____ Theft; _____ Loss; _____ Improper Disposal; _____ Unauthorized Access;

_____ Hacking/IT Incident; _____ Other - Explain _____________________________

_____ Unknown  
If “Other” is checked, please explain

Location of Breached Information at the Time of the Breach (Check where appropriate)

_____ Laptop; _____ Desktop Computer; _____ Network Server; _____ e-Mail;

_____ Other Portable Electronic Device; _____ Electronic Medical Record;

_____ Paper; _____ Oral; _____ Other – Explain _____________________________

If “Other” is checked, please describe the location of the Breached Information below:

Type of Protected Health Information Involved in the Breach (Check where appropriate)

_____ Name; _____ Address/Zip; _____ Date of Birth; _____ Social Security Number;

_____ Driver’s License Number; _____ Other Identifier; _____ Medical Record Number;

_____ Diagnoses/Conditions; _____ Medications; _____ Lab results;

_____ Physician/Operative reports; _____ Radiology results;

_____ Financial Information; _____ Credit Card/Bank Acct #;

_____ Insurance Claims Information; _____ Other Financial Information; _____ Other;

If “Other” is checked, please describe the Breached Information in detail below:
**Brief Description of the Breach**: Please include a description of the Breach, how the Breach occurred, and any additional relevant information regarding the type of Breach, type of media, and type of protected health information involved in the Breach. Also, please identify any employees, agents or contractors associated with the Breach and the extent to which each are involved:

**Safeguards in Place Prior to the Breach**

- Firewalls; 
- Secure Browser Sessions; 
- Passwords; 
- Encrypted Wireless; 
- Encryption in place; 
- Anti-virus software; 
- Intrusion detection; 
- Biometrics (e.g. eye, thumb print); 
- Physical Security (security alarm, locked cabinet); 
Please specify: 

If “Other” is checked, please describe the safeguards in detail below:

**Actions Taken in Response to the Breach**:

- Security and/or Privacy Safeguards
- Mitigation
- Sanctions
- Policies and Procedures
- Other

If “Other” is checked, please describe the actions taken in response to the Breach in detail below:
POLICY REGARDING MONITORING, ACTIVITY REVIEW, AND AUDITING OF INFORMATION SYSTEMS

POLICY: SB Clinical Network IPA, LLC, doing business as Suffolk Care Collaborative Performing Provider System (the “Suffolk PPS”), implements appropriate hardware, software or procedural auditing mechanisms on electronic protected health information (“e-PHI”) systems and reviews records of activity generated by the auditing mechanisms on an ongoing basis.

PROCEDURES:

A. Information Systems Activity Review.

1. e-PHI Systems have the appropriate hardware, software or procedural auditing mechanisms installed to enable review of information system activity on an ongoing basis. These mechanisms generate at a minimum the following information about information systems activity:

   a. date and time of activity; *refer to notation below
   b. description of attempted or completed activity;
   c. identification of user performing activity; and
   d. origin of activity (e.g., I/P address, workstation ID).

2. When feasible e-PHI Systems have the appropriate hardware, software or procedural auditing mechanisms installed to generate reports of auditable events such as:

   a. failed authentication attempts;
   b. access to sensitive e-PHI (e.g., e-PHI regarding all affected employees and persons associated with the Suffolk PPS, including executives, governing body members and Coalition Partners);
   c. information system start-up or shutdown;
   d. use of privileged accounts (e.g., system admin account); and
   e. security incidents.

3. The contracted Cloud Service Provider (CSP) of the Healthe Intent Platform has the appropriate auditing mechanisms installed to enable review of information system activity on an ongoing basis. These mechanisms generate at a minimum the following information about information systems activity:

   a. server alerts and error messages;
   b. user log-on and log-off (successful or unsuccessful);
   c. all systems administration activities;
   d. modifications of privileges and access;
   e. start up and shut down;
   f. application modifications;
g. application alerts and error messages;

h. configuration changes;

i. account creation, modification or deletion;

j. file creation and deletion;

k. read access to sensitive information;

l. modification to sensitive information and

m. printing sensitive information

4. Audit mechanisms are implemented and reviewed on all e-PHI Systems on an ongoing basis. The audit mechanism review process includes, but is not limited to:

   a. definition of what activity is significant;
   b. procedures for defining how significant activity is identified and, if appropriate, reported;
   c. procedures for maintaining the integrity of records of significant activity;
   d. identification of individuals authorized to review records of activity; and
   e. definition of activity records archiving and retention processes and procedures.

4. Suffolk PPS’ Information Privacy and Security Officer or designee respond to information security incidents and provide remedial technical and administrative measures in response to an incident.

5. The audit tool and audit data/information are protected from unauthorized access, modification and deletion. Access to create an audit report is restricted to two Stony Brook Medicine Information Technology (SBMIT) staff who are not otherwise permitted to access the system.

6. Any discrepancies found are reported to the SCC Information Privacy and Security Office for investigation and appropriate corrective processes.

7. Access audit logs are maintained in accordance with applicable Record Retention Policies

**Information Systems Audit.**

3. Suffolk PPS’ Information Privacy and Security Officer ensures that annual evaluations of security safeguards, including policies, controls and processes are conducted and adequately documented.

4. Evaluations may include:

   a. a review of Suffolk PPS’ security policies and procedures to evaluate their appropriateness and effectiveness in protecting against any reasonably anticipated threats or hazards to the confidentiality, integrity and availability of e-PHI;
   
   b. a gap analysis to compare Suffolk PPS’ security policies and procedures against other entities or industry standards;

   c. an identification of threats, and risks to e-PHI and e-PHI Systems, in accordance with Suffolk PPS’ e-PHI policy regarding risk analysis and management;

   d. an assessment is made of Suffolk PPS’ security controls to determine if such processes are reasonable and appropriate to provide protection against the risks identified for e-PHI Systems; and
e. technical and non-technical testing and evaluation of Suffolk PPS’ security controls and processes is done to determine whether the controls have been implemented properly and appropriately protect e-PHI.

5. The evaluation results are documented in a written report and provided to the Information Privacy and Security Officer who presents the results to Suffolk PPS executive staff for review, approval and appropriate action.

6. After an initial evaluation is completed to determine the extent of compliance with the standards implemented under the Health Insurance Portability and Accountability Act 1996 (“HIPAA”) Security Regulations, subsequent periodic reevaluations are conducted in response to environmental or operational changes occurring since the last evaluation that might impact the confidentiality, integrity or availability of e-PHI. Changes that may trigger a reevaluation of Suffolk PPS’ security safeguards include:

   a. known security incidents;
   b. new threats or risks to security of e-PHI;
   c. changes to Suffolk PPS’ organizational or technical infrastructure;
   d. changes to information security requirements or responsibilities; and
   e. new security technologies that are available and new security recommendations.

7. Following each evaluation, Suffolk PPS updates its security policies, procedures, controls and processes as necessary in order to protect against any reasonably anticipated threats or hazards to the confidentiality, integrity and availability of e-PHI or to otherwise enhance compliance with the HIPAA Security Regulations.

B. **Disciplinary Action.** Suffolk PPS’ Information Privacy and Security Officer has general responsibility for implementation of this policy. Individuals who violate this policy are subject to disciplinary action in accordance with Suffolk PPS policies and procedures, up to and including termination of employment or contractual relationship with Suffolk PPS.

C. **Policy Review:** This policy is reviewed at least annually by the Suffolk PPS’s Information Privacy and Security Officer, or designee. This policy may be amended from time to time at the Suffolk PPS’s discretion.

D. **Coalition Partners.** Each Coalition Partner is responsible for implementing policies and procedures regarding monitoring, activity review, and auditing of information systems internally. Each Coalition Partner is independently responsible for ensuring that its internal employees, independent contractors, executives and governing board members are aware of and comply with such policies and procedures.

*audit log date/time stamps must be generated from the internal system clock that can be mapped to Greenwich Mean Time (GMT) and is accurate within thirty (30) seconds. The system is set-up to compare the internal clock at least daily and upon system boot against NIST Internet Time Servers (http://tf.nist.gov/tf-cgi/servers.cgi) as the authoritative time source and synchronize the internal clock to the authoritative time source with the time difference is greater than thirty (30) seconds.

**refer to SUNY Retention Schedule for Health Information found at:**
http://system.suny.edu/media/suny/content-assets/documents/compliance/info-management/records/Health-Information.pdf
SUFFOLK CARE COLLABORATIVE

POLICY REGARDING RISK ANALYSIS AND MANAGEMENT OF PROTECTED HEALTH INFORMATION

POLICY: SB Clinical Network IPA, LLC, doing business as Suffolk Care Collaborative performing provider system (the “Suffolk PPS”), recognizes the importance of implementing physical, technical, and administrative safeguards to ensure confidentiality, integrity and availability of protected health information and electronic protected health information (collectively referred to herein as “PHI”). Suffolk PPS conducts risk analyses and manages risks to ensure the confidentiality, integrity and availability of PHI on an ongoing basis.

PROCEDURES:

A. Suffolk PPS conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of PHI, and also implement security risk measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the provisions of the Health Insurance Portability and Accountability Act 1996 (“HIPAA”) and other applicable confidentiality, privacy and security regulations.

B. The risks to the confidentiality, integrity and availability of PHI is identified and prioritized on an ongoing basis. A documented risk analysis process is used as the basis for identification, definition and prioritization of risks to PHI.

C. The risk analysis is conducted annually and reviewed on an ongoing basis and used in conjunction with a risk management process. An update to the risk analysis is conducted when environmental or operational changes have occurred that impact the confidentiality, integrity or availability of PHI.

D. Suffolk PPS designates individuals to implement, monitor and audit Suffolk PPS’ PHI risk analysis process and management.

E. The risk management process implemented by Suffolk PPS is based on a documented process that is used as a basis for selection and implementation of the security measures as determined in the risk analysis. The risk management process includes the following:

1. Assessment and prioritization based on Suffolk PPS executive staff approval, on the basis of risks to PHI Systems.

2. Selection and implementation of reasonable, appropriate and cost-effective security measures to manage, mitigate or accept identified risks.

3. Security training and awareness on implemented security measures to all affected employees and persons associated with the Suffolk PPS, including executives and governing body members.
4. Ongoing evaluation and revision of security measures, as necessary.

F. The risk management process are used as the basis for the identification, definition and prioritization of risks to PHI. The risk analysis process includes the following:

1. identification and prioritization of the threats to PHI;
2. identification and prioritization of the vulnerabilities of PHI;
3. identification of a probable threat that may exploit the vulnerability of PHI;
4. identification and definition of measures used to protect the confidentiality, integrity and availability of PHI;
5. identification of new threats or risks that impact PHI;
6. identification of a new security incident that impacts PHI;
7. changes to Suffolk PPS information security requirements or responsibilities that could impact PHI; and
8. changes to the organizational or technical infrastructure that could impact PHI.

G. Review of Policy/Procedure as relates to risk: In the event of a significant regulatory change or on an annual basis this policy is reviewed and updated as needed to ensure its effectiveness in complying with the HIPAA Security Regulations.

H. Suffolk PPS and Suffolk PPS’ Information Privacy and Security Officer have the general responsibility for implementation and enforcement of this policy.

I. Each Coalition Partner is responsible for implementing policies and procedures regarding risk analysis and management of PHI internally. Each Coalition Partner is independently responsible for ensuring that its internal employees, independent contractors, executives and governing board members are aware of and comply with such policies and procedures.
SUFFOLK CARE COLLABORATIVE

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)
TRAINING POLICY

POLICY: SB Clinical Network IPA, LLC, doing business as Suffolk Care Collaborative performing provider system (the “Suffolk PPS”), recognizes the importance of educating affected employees and persons associated with the Suffolk PPS, including executives and governing body members, on patient confidentiality policies and procedures, the provisions of the Health Insurance Portability and Accountability Act 1996 (“HIPAA”) and other applicable confidentiality, privacy and security regulations. Suffolk PPS ensures that individuals and entities participating in or do business with Suffolk PPS, including but not limited to (i) Suffolk PPS and its employees, independent contractors, vendors, agents, suppliers, executives and governing body members; and (ii) all Coalition Partners and their employees, independent contractors, vendors, agents, suppliers, executives and governing body members (“PPS Associates”) are educated on the patient privacy and confidentiality issues related to Suffolk PPS operations and/or the Delivery System Reform Incentive Payment (“DSRIP”) program.

PROCEDURES:

A. **Training.** All affected employees and persons associated with the Suffolk PPS, including executives and governing body members receive HIPAA awareness training including relevant policies and procedures at the time of hire (new employee orientation), annually thereafter as part of the mandatory/required training program and periodically throughout the year as necessary/required. The format includes such methods as web-based training module, large and small group in-person presentation(s), and large and small group web presentations as deemed appropriate or upon request.

Training includes but is not limited to Suffolk PPS policies and procedure addressing the confidentiality of patient information, administrative simplification, HIPAA Privacy, HIPAA Security (administrative, physical and technical safeguards) and relevant New York State confidentiality regulations (public health, mental hygiene, HIV, genetics and minors).

B. **Security Reminders and Re-Education.** The Information Privacy and Security Officer is responsible for communicating updates and regulatory amendments that occur during the course of the calendar year via e-mail, distributed newsletter, posted publications, added to subsequent training activities, or any other method at the discretion of the Information Privacy and Security Officer, as necessary for dissemination.

C. **Policy Review.** At a minimum this policy is reviewed annually by the Suffolk PPS’s Information Privacy and Security Officer, or designee. This policy may be amended from time to time at Suffolk PPS’s discretion.

D. **Coalition Partners.** Each Coalition Partner is responsible for implementing this Policy internally. Each Coalition Partner is independently responsible for ensuring that its internal employees, independent contractors, executives and governing board members receive training and re-education, as needed and
certify compliance with the training requirement. Failure to comply with training requirements may result in disciplinary action up to and including termination or exclusion.
SUFFOLK CARE COLLABORATIVE

Information Security System and Communication Protection Policy

POLICY: SB Clinical Network IPA, LLC, doing business as Suffolk Care Collaborative (SCC) performing provider system (the “Suffolk PPS”), maintains an enterprise system and communications protection program for managing risks from vulnerable system configurations, denial of service, data communication and data transfer. The system and communication program ensures Suffolk PPS partners implement security best practices with regard to system configuration, data communication and data transfer.

PROCEDURES:

A. Program Requirements

1) Each Suffolk PPS partner adheres to a documented system and communication protection process and implements security best practices with regard to system configuration, data communication and data transfer.

2) All Suffolk PPS partners separate system user functionality, including user interface services, from information asset management functionality.

3) All Suffolk PPS partners systems isolate security functions from non-security functions.

4) All Suffolk PPS partners implement measures to prevent unauthorized and unintended information transfer via share system resources.

5) All Suffolk PPS partners implement measures to protect against or limited the effects of denial of services attacks.

6) All Suffolk PPS partners monitor and control communications at the external boundary of the system and significant internal boundaries with the system. All Suffolk PPS partners connect to external networks or information assets through secure managed interfaces.

7) All Suffolk PPS partners implement appropriate transmission protocols for the secure transmission of data to protect the confidentiality and integrity of the data.
8) All Suffolk PPS partners terminate network connectivity associated with a communications session at the end of the session or following 15 minutes of inactivity.

9) All Suffolk PPS partners implement appropriate encryption mechanisms to prevent unauthorized disclosure and integrity of data during storage and transmission. The encryption key is generated, distributed, stored, accessed and destroyed in accordance with industry best practices.

10) All Suffolk PPS partners protect information systems from public access and/or availability to protect the integrity of the systems.

11) Collaborative computing devices are prohibited.

12) Public Key certificates are prohibited.

13) All Suffolk PPS partners identify acceptable mobile code and mobile code technologies and implement user restrictions for unacceptable mobile code and mobile code technologies.

14) All Suffolk PPS partners employing voice over internet protocol (VoIP) technology establishes user restrictions and implementation guidelines to protect the confidentiality, integrity and availability of information systems.

15) Secure Name/Address Resolution Architecture and Provisioning Service (Authoritative Source, Recursive or Caching Resolver) use of redundant/fault-tolerant system for DNS queries within the network prohibiting name resolution to external parties.

16) Suffolk PPS partners will protect session authenticity between communications to ensures that data in transmission is not hi-jacked or altered.

17) Suffolk PPS partners will ensure fail in known state through encryption of data at rest and back-up to either a redundant secure server or cloud storage solution.

B. **Disciplinary Action.** Suffolk PPS’ Information Privacy and Security Officer has general responsibility for implementation of this policy. Individuals who violate this policy are subject to disciplinary action in accordance with Suffolk PPS policies and procedures, up to and including termination of employment or contractual relationship with Suffolk PPS.

C. **Policy Review:** This policy is reviewed at least annually by the Suffolk PPS’s Information Privacy and Security Officer, or designee. This policy may be amended from time to time at the Suffolk PPS’s discretion.

D. **Coalition Partners.** Each Coalition Partner is responsible for implementing policies and procedures regarding monitoring, activity review, and auditing of information systems internally. Each Coalition Partner is independently responsible for ensuring that its internal employees,
independent contractors, executives and governing board members are aware of and comply with such policies and procedures.
SUFFOLK CARE COLLABORATIVE

Wireless Networking

Policy: SB Clinical Network IPA, LLC, doing business as Suffolk Care Collaborative (SCC) performing provider system (the “Suffolk PPS”), ensures the wireless networking infrastructure is properly controlled, configured and administered in a secure manner.

Definitions:

Network Infrastructure - the physical hardware used to transmit data electronically such as routers, switches, gateways, bridges, and hubs

Procedures:

A. Administration: Stony Brook Medicine Information Technology (SBMIT) Network Support Services is responsible for the oversight, appropriate use and/or management of all Suffolk PPS wireless network installations.

B. Wireless Networking Request: Any member of Suffolk PPS wanting to use wireless networking within their building or department can submit a service request to arrange for a site survey by SBMIT Network Support Services to assess the requirements for wireless connectivity. The service request is submitted by calling 444-HELP.

C. Equipment Purchases: SBMIT Network Support Services provides to the requestor a list of approved manufacturers, models, number of units and required hardware to be purchased in order to integrate with the Suffolk PPS wireless network infrastructure. Wireless hardware that is installed and either is not inspected by SBMIT Network Support Services or does not conform to Suffolk PPS wireless requirements is identified and disconnected from the network.

D. Acquisition: The requestor is responsible for purchasing the wireless equipment when the request is outside of the scope of Suffolk PPS Wireless Initiatives. SBMIT Network Support Services as the agent for Suffolk PPS is the only party to install and manage wireless equipment.

E. Legacy equipment: For members of Suffolk PPS with legacy non-standard wireless access point installed prior to the establishment of the Suffolk PPS Wireless Networking policies, SBMIT Network Support Services conducts a site survey to assess the coverage radius, security policy
and document all relevant settings associated with the access point. When SBMIT Network Support Services determines that the access point cannot be configured to comply with Suffolk PPS Wireless Networking policies the members of Suffolk PPS responsible for the unit are required to purchase compliant hardware within 30 days or have an implementation plan approved by SBMIT Network Support Services. All remaining non-compliant, non-standard wireless hardware is disconnected from the network until compliant hardware is purchased.

F. Security: All Suffolk PPS wireless networks employ the most current security policies as approved by SBMIT Network Support Services for authentication, access control and encryption, such as (RADIUS, WEP or WPA). Failure to follow this policy results in wireless devices being disconnected from the wireless network until there is compliance.

G. Audits: SBMIT Network Support Services conducts and/or requests copies of regular surveys and network system log monitoring to ensure compliance with this policy.

H. Disciplinary Action. Suffolk PPS’ Information Privacy and Security Officer has general responsibility for implementation of this policy. Individuals who violate this policy are subject to disciplinary action in accordance with Suffolk PPS policies and procedures, up to and including termination of employment or contractual relationship with Suffolk PPS.

I. Policy Review: This policy is reviewed at least annually by the Suffolk PPS’s Information Privacy and Security Officer, or designee. This policy may be amended from time to time at the Suffolk PPS’s discretion.

J. Coalition Partners. Each Coalition Partner is responsible for implementing policies and procedures regarding monitoring, activity review, and auditing of information systems internally. Each Coalition Partner is independently responsible for ensuring that its internal employees, independent contractors, executives and governing board members are aware of and comply with such policies and procedures.
POLICY REGARDING MULTIFACTOR AUTHENTICATION (MFA) FOR ACCESS TO IDENTIFIABLE PATIENT DATA VIA HEALTHEINTENT APPLICATION

POLICY: SB Clinical Network IPA, LLC, doing business as Suffolk Care Collaborative (SCC) performing provider system (the “Suffolk PPS”), implements the appropriate multifactor authentication for user access to identifiable patient information available within the HealtheIntent platform.

A. The SCC relationship manager is responsible for identifying PPS downstream partners who require a realm administrator (RA) for their organization. The RA are responsible for Identity Assurance management and the administration of secure tokens that are required for Multi Factor Authentication (MFA). MFA is required for all end user access to the SCC HealtheIntent Platform. The operational process is as follows:

The SCC relationship manager notifies SCC Enterprise Realm Administrator (ERA) each time a new RA has been identified. The SCC ERA delegates Identity Assurance (IA) processes to the PPS Partners RA. The SCC ERA provisions and authorizes the PPS partner’s RA to perform the IA processes (on the behalf of the SCC) within the given PPS partner’s organization. Upon successful completion of the IA processes the RA provisions the MFA tokens to specific authorized users within PPS partner’s organization.

The SCC relationship manager is responsible for working with each RA to identify the specific set of authorized users within the PPS partners’ organization requiring access to the SCC HealtheIntent Platform.

Note: SCC MFA tokens can only be used to access the Stony Brook Hub HealtheIntent Platform and cannot be used to access other applications within the PPS Partners organizations.

Once the PPS Partners RA has completed issuing secure tokens the SCC relationship manager is notified by the RA that the IA and secure token provisioning processes have been completed. The RA provides a list of authorized users to the SCC relationship manager. Each authorized user is then identified by name, title, credentials, level of access and employee ID # (if applicable) by the SCC relationship manager on the HealtheIntent Application User Provisioning Request Form.

B. The SCC ERA conducts the IA and provisioning of MFA tokens for small PPS Partners with only a few users requiring access to the HealtheIntent platform.
In these cases the SCC ERA is responsible for performing the same steps that are outlined above for the PPS Partners RA.

C. Each authorized individual requiring access is validated by the PPS Partner RA as follows:

2. Signed Confidentiality Agreement.
3. Presented appropriate photo ID at the time of MFA distribution.

D. HealtheIntent authorized Stony Brook Medicine (SBM) individuals with existing MFA for e-prescribing issued through Stony Brook Medicine Information Technology (SBMIT) present to HealtheIntent (HealtheCare, HealtheRegistries, HealtheEDW) training with their SBM ID and will have their current token processed to add access to the HealtheIntent platform.

E. HealtheIntent authorized individuals who are not e-prescribers present to HealtheIntent (HealtheCare, HealtheRegistries, HealtheEDW) training with their federal or state issued photo ID and are issued an appropriate token for which is required to access HealtheIntent platform.

F. Multi Factor authentication is required for all user access to the HealtheIntent platform. Authorized individuals gain access the HealtheIntent applications (HealtheCare, HealtheRegistries, HealtheEDW) through an authentication protocol that uses the following two factors:

1. Something the individual knows such as a username/password, and
2. Something the individual has such as a security device, hard token or smartphone soft token app

G. HealtheIntent authorized individuals are prohibited from sharing usernames/passwords and security tokens.

H. HealtheIntent authorized individuals log off workstations and mobile devices prior to walking away and/or leaving a workstation or device unattended. The use of another person’s access rights (log on credentials, username/password and/or token) is a violation of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule and New York State Cyber Information Security Policy.

I. Procedures related to unsuccessful system access attempts, account disabling and auditing/monitoring are found in the SCC HIPAA Policy #5 Regarding ID and Password Assignment for Computer System Access.

J. HealtheIntent authorized individuals’ MFA access to the HealtheIntent application(s) (HealtheCare, HealtheRegistries, HealtheEDW) is promptly disabled or revoked and hard token returned to the PPS Partner Administrator whenever the following occurs:
1. When the user’s access credentials and/or hard/soft token are reported lost, stolen or compromised.
2. When the user role changes or practitioner license is suspended/revoked.
3. When the user employment is terminated with the organization engaged in SCC/DSRIP business.

K. The SCC off-boarding process requires the identification and submission of notice from the PPS Partner Administrator regarding the termination/separation of individual(s) with HealtheIntent access. Access to the HealtheIntent platform is promptly revoked/disabled upon receipt of notice for any individual no longer affiliated with SCC or a PPS Partner.

L. Replacement tokens:

1. For HealtheIntent authorized individuals with MFA access to the HealtheIntent platform to obtain a replacement hard token, the individual must present in person to the PPS Partner Administrator with their photo ID for validation to obtain a new token.
2. For HealtheIntent authorized individuals with MFA access to the HealtheIntent platform wishing to switch from a hard token to a soft token, the individual must present in person to the PPS Partner Administrator with their photo ID for validation, their smart phone and their hard token in exchange for the soft token app download onto their smartphone.
3. For the HealtheIntent authorized individuals with MFA access to the HealtheIntent platform to obtain a replacement soft token (new smart phone, lost/misplaced soft token download instruction document) the individual must present in person to the PPS Partner Administrator with their photo ID for validation to obtain a new soft token app download.

M. Disciplinary Action. Suffolk PPS’ Information Privacy and Security Officer has general responsibility for implementation of this policy. Individuals who violate this policy are subject to disciplinary action in accordance with Suffolk PPS policies and procedures, up to and including termination of employment or contractual relationship with Suffolk PPS.

N. Policy Review: This policy is reviewed at least annually by the Suffolk PPS’s Information Privacy and Security Officer, or designee. This policy may be amended from time to time at the Suffolk PPS’s discretion.

O. Coalition Partners. Each Coalition Partner is responsible for implementing policies and procedures regarding monitoring, activity review, and auditing of information systems internally. Each Coalition Partner is independently responsible for ensuring that its internal employees, independent contractors, executives and governing board members are aware of and comply with such policies and procedures.
POLICY AND REGULATORY VIOLATIONS AND DISCIPLINARY PROCESS

POLICY: SB Clinical Network IPA, LLC, doing business as Suffolk Care Collaborative performing provider system (the “Suffolk PPS”), takes appropriate action, including but not limited to disciplinary action, against any individual who violate a SCC policy and/or applicable state or federal confidentiality laws. This policy specifically refers to compliance with 45 CFR §160 and 164 the Health Insurance Portability and Accountability Act 1996 (HIPAA) and amendments to HIPAA under the 2013 Omnibus Rule including Breach Notification provisions; New York State Public Health Law Article 27-F Confidentiality of HIV and HIV Related Information, New York State Mental Hygiene Law §33.13, Genetic Information Non-Discrimination Act (GINA) and where applicable 42 CFR Part 2 Confidentiality of Alcohol and Drug Abuse Patient Record for access to and the receipt, maintain, transmission and storage of information protected under these policies and laws.

PROCEDURES:

A. All individuals with access to DSRIP data will be monitored for appropriateness of their access activities.

B. Unusual and/or unauthorized access activities are reported to the Suffolk PPS’s Information Privacy and Security Officer.

C. The Suffolk PPS’s Information Privacy and Security Officer conducts a thorough assessment of the access activities reported to determine if the access is unusual and/or unauthorized.

D. Upon a determination inappropriate/unauthorized access by the Suffolk PPS’s Information Privacy and Security Officer prompt notification to the designated PPS Administrator and access termination measures are taken.

E. Further consideration of the inappropriate/unauthorized access includes potential sanctions and/or appropriate disciplinary measures (refer to section below) and a breach risk assessment to determine if the affected patients confidentiality has been compromised requiring notification to the affected individual(s).

F. Levels of Violations:

Level I - Accidental and/or due to lack of proper education or training. Careless or unintentional Use or disclosure of PHI without a legitimate need to know the patient information: examples include, but are not limited to, discussing patient information in a public area, leaving a copy Of a patient medical information in an area open to public access, leaving a computer containing Medical information unattended and therefore, unsecured, accessing one’s own medical record And accessing the medical record of a minor child for whom you are a legal guardian.
Level II – Curiosity or concern (no personal gain). Intentional access or discussion of patient Information with purposes other than the care of the patient or other authorized use but for Reasons unrelated to personal gain: examples include, but are not limited to, looking up birth Dates, addresses of friends/relatives/colleagues, accessing and reviewing a medical record or other Health information of a friend/relative/colleague without proper authorization.

LEVEL III – Personal gain or malice. Intentional access, review, discussion or distribution of Patient information for personal gain or with malicious intent: examples include, but are not Limited to, reviewing a patient medical record to use information in a personal relationship, Compiling a mailing list for personal use or to be sold, and inappropriately providing information To the media.

G. Levels of Sanction:

1. Oral warning in the form of re-education
2. Verbal or Written Counseling
3. Attendance and successful completion of additional training or Educational program
4. Regular/more frequent monitoring of PHI access activities
5. Disciplinary action to include a range of penalty from fines up to Suspension/termination.

H. Disciplinary Action. Suffolk PPS’ Information Privacy and Security Officer has general responsibility for implementation of this policy. Individuals who violate this policy are subject to disciplinary action in accordance with Suffolk PPS policies and procedures, up to and including termination of employment or contractual relationship with Suffolk PPS.

I. Policy Review: This policy is reviewed at least annually by the Suffolk PPS’s Information Privacy and Security Officer, or designee. This policy may be amended from time to time at the Suffolk PPS’s discretion.

J. Coalition Partners. Each Coalition Partner is responsible for implementing policies and procedures regarding monitoring, activity review, and auditing of information systems internally. Each Coalition Partner is independently responsible for ensuring that its internal employees, independent contractors, executives and governing board members are aware of and comply with such policies and procedures.
Electronic Information Access Confidentiality Certification

Important: Please read all sections. If you have any questions; have them answered before signing.

1. Confidentiality of Patient Information:

   a) All patient health information is private and confidential therefore access to this information is a privilege that must not be taken for granted.

   b) Patients provide personal information with the expectation that it will be kept confidential and only be used by authorized persons as necessary to provide treatment, obtain payment for services provided and to perform other business related activities necessary to maintain appropriate health care operations;

   c) All personally identifiable information provided by patients or regarding medical services provided to patients, including oral, written, printed, photographic and/or electronic (collectively the “Confidential Information”) is strictly confidential and is protected by federal and state confidentiality laws and regulations including but not limited to the Health Insurance Portability and Accountability Act 1996 (HIPPA) that prohibit its unauthorized use or disclosure;

   d) For the duration of my affiliation with Suffolk Care Collaborative (SCC), I may be given access to certain Confidential Information that may also require additional protections including but not limited to:

      1) The New York State Public Health Law Article 27-F and Part 63 of 10 NYCRR AIDS Testing and Confidentiality of HIV-Related Information; which states that no person who obtains confidential HIV-related information in the course of providing any health or social service or pursuant to a release of confidential HIV-related information; including but not limited to any information indicating that a person has had an HIV-related test, such as an HIV antibody test; has HIV-infection, HIV-related illness, or AIDS; or has been exposed to HIV, may disclose or be compelled to disclose such information. Illegal disclosure of confidential HIV-related information may be punishable by a fine of up to $5,000 and a jail term of up to one year

      2) New York State Mental Hygiene Law § 33.13 governs the protection, confidentiality and disclosure of behavioral health services, psychiatric care and substance abuse treatment. The law strictly limits disclosure of mental hygiene related information. All disclosures of mental hygiene related information require an authorization signed by the patient/individual or their personal representative.

2. Disclosure, Use and Access of Electronic or Hard Copy Confidential Information:

Any information acquired or accessed through my affiliation with SCC must be kept confidential. This applies to all HIPAA Protected Health Information (HIPAA-e-PHI) and includes but is not limited to patient information, participate organization proprietary information and confidential business information pertaining to SCC.

Each individual who is permitted access to SCC is responsible for protecting the privacy of the patients’ information that is accessible through the network. Individuals with access to SCC must also take care to preserve confidentiality of such information in conversations, in handling, copying, storing, and disposal of documents and any and all electronic media that contains such information.
Access to SCC system and other proprietary or SCC business related information is permitted on an as needed basis. Access is granted based on the individual’s job title, position or assigned responsibilities and does not allow access to any information that is not part of one’s duties and responsibilities.

Each individual who is permitted access to SCC will receive a username and temporary password for accessing the SCC system. Each individual who is granted access is responsible for maintaining confidentiality of the information contained in the SCC system by never sharing their password or allowing others to use their access and always locking or logging off the SCC system prior to leaving the workstation, PC, laptop or other electronic device used to access the SCC system, unattended. Each individual who is granted access to the SCC system is accountable for any and all activities that occur under their username and password. This activity will be periodically monitored.

Disclosure of confidential information is prohibited even after termination of affiliation with or access to SCC; either as a member of a participating organization which has terminated the participation agreement or as an individual who is no longer affiliated with a participating organization, unless specifically waived in writing by an authorized party who has consulted with SCC Legal Counsel and/or the SCC Information Privacy and Security Officer.

I agree, that except as authorized in connection with my assigned duties, I will not at any time use, access or disclose any Confidential Information to any person (including, but not limited to co-workers, friends and family members). I understand that this obligation remains in full force during the entire term of my affiliation with or access to SCC system and continues in effect after such affiliation or access is terminated.

3. Confidentiality Policy

I agree, I will comply with federal and state confidentiality laws as well as SCC policies and procedures that apply to me as a result of my affiliation with or access to SCC systems. Any violation of this acknowledgement or SCC policies and procedures is strictly prohibited.

4. Return of Confidential Information

Upon termination of my affiliation with or access to SCC systems, for any reason, or at any other time upon request, I agree to promptly return to SCC or my participating organization SCC administrator any copies of Confidential Information obtained through the SCC system in my possession or control (including all printed and electronic copies), unless retention is specifically required by law or regulation.

5. Periodic Certification

I understand that I will be required to periodically certify that I have complied in all respects with this Acknowledgment, and I agree to so certify upon request.

6. Remedies

I understand and acknowledge that the restrictions and obligations I have accepted under this Acknowledgement are reasonable and necessary in order to protect the interests of the patients who have consented to allow their health information be made available to me through SCC and that my failure to comply with this Acknowledgement in any respect could cause irreparable harm to patients, SCC and/or my employer.

7. Violations

I understand that SCC may initiate administrative actions against me in accordance with SCC policies and procedures or applicable federal or state laws for disclosure of or unauthorized use of patient health information or proprietary SCC business information or non-compliance with this acknowledgement. I understand that SCC sanctions for a violation may include, but are not limited to, penalties up to and including termination affiliation with SCC and/or access to SCC system. I understand that I may be subject to civil and/or criminal penalties as well in accordance with federal or state laws.
I have received and read this Statement of Confidentiality and understand the requirements set forth in it.

Printed Name (LEGIBLY):______________________________________ Date: ______________

Signature: ________________________________ Employee ID #: ______________ (if applicable)
My signature on this sheet acknowledges my attendance at the above titled training program. I have received information as applicable to my responsibilities pertaining to the access and use of the SCC/DSRIP system and SCC policies and procedures. I agree to maintain the standards presented in this training and to comply with the SCC Policies and Procedures.

<table>
<thead>
<tr>
<th>Print Name Legibly</th>
<th>Signature</th>
<th>Employee ID Number (from ID Badge)</th>
<th>Department/Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

All of the above noted staff have received and successfully completed training, including but not limited, to the proper access and use of the SCC System, confidentiality of the information accessed through the SCC/DSRIP System, security procedures to protect and maintain the integrity of the information and SCC Policies and Procedures.

____________________________________  ____________________________________________
Designated SCC Site Administrator (Print Name)  Designated SCC Site Administrator (Signature)
User Account Request Form

Facility_________________________ Date________________________

User Account Role Levels:

1 – Practitioner with access to clinical information
2 – Non-Practitioner with access to clinical information
3 – Non-Practitioner with access to non-clinical/aggregate information only
4 – SCC Administrator(s) with access to non-clinical/aggregate information only
5 – SCC Administrator(s) with access to clinical information for public health reporting only

Please fill in the chart below completely for staff access to the SCC Healthe Intent Platform.

►All information must be typed and NOT hand-written. Forms not typed will not be accepted.

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Credentials (RN, MD, NP, PA, etc)</th>
<th>User Acct Role Level (1-5)</th>
<th>Employee ID # (if applicable)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Certification by site designated SCC Site-Administrator:

I hereby certify that the above listed staff credentials are accurate as verified and maintained by my facility; and the access requested is in compliance with SCC policies and procedures.

______________________________  ________________________________
SCC Site-Administrator           SCC Site-Administrator
Print Name                      Signature
Information Security Plan

The Information Security Plan (ISP) establishes and states the policies and procedures governing Suffolk Care Collaborative (SCC) standards and practices. The policies express SCC goals for managing and controlling the privacy and security of Information Systems (IS) used by SCC, its Performing Provider System (PPS) Partners, New York State Department of Health (NYSDOH) Medicaid Analytics Performance Portal (MAPP), and Business Associates in the operations of the Delivery System Reform Incentive Payment (DSRIP) Program. The ISP represents the processes and guidelines for achieving and maintaining these standards and practices as well as compliance with federal and state regulations.

Approved by the SCC Information Security Task Force October 2015
Last review by the Chief Information Privacy & Security Officer 5/17/2017
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>Page 3</td>
</tr>
<tr>
<td>Purpose</td>
<td>Page 3</td>
</tr>
<tr>
<td>Scope</td>
<td>Page 4</td>
</tr>
<tr>
<td>Definitions</td>
<td>Page 4 - 7</td>
</tr>
<tr>
<td>IT Governance Commitments &amp; Responsibilities</td>
<td>Page 7</td>
</tr>
<tr>
<td>SCC Policy Statement</td>
<td>Page 8</td>
</tr>
<tr>
<td>Enforcement</td>
<td>Page 8</td>
</tr>
<tr>
<td>Information Security Program</td>
<td>Page 8</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>Page 9</td>
</tr>
<tr>
<td>Control Activities (Internal, Preventative, Detective and Corrective)</td>
<td>Page 9 - 11</td>
</tr>
<tr>
<td>Stony Brook Medicine Information Security Policy</td>
<td>Page 11</td>
</tr>
<tr>
<td>Organization of Information Security</td>
<td>Page 11 – 12</td>
</tr>
<tr>
<td>Accountability for Assets</td>
<td>Page 12</td>
</tr>
<tr>
<td>Information Classification</td>
<td>Page 13 - 14</td>
</tr>
<tr>
<td>Identity and Access Management</td>
<td>Page 14 - 18</td>
</tr>
<tr>
<td>Communication and Operations Management</td>
<td>Page 18 - 20</td>
</tr>
<tr>
<td>Systems &amp; Application Security</td>
<td>Page 20 – 23</td>
</tr>
<tr>
<td>Physical Security Measures</td>
<td>Page 23 – 24</td>
</tr>
<tr>
<td>Business Continuity</td>
<td>Page 25 – 26</td>
</tr>
<tr>
<td>Information Security Incident Response</td>
<td>Page 26</td>
</tr>
</tbody>
</table>

**Attachments:**
- Related Policies and Procedures
- Confidentiality Agreements
- Account Request Forms
Executive Summary

Stony Brook University Hospital (SBUH) is the Performing Provider System Lead (PPS Lead) for the Delivery System Reform Incentive Payment (DSRIP) Program contract awarded by New York State to SB Clinical Network IPA, LLC, doing business as a PPS, the Suffolk Care Collaborative (SCC). The SCC is also known colloquially as the Suffolk PPS.

SCC has engaged the Information Technology department of SBUH, known as Stony Brook Medicine IT (SBMIT) as a Business Associate to oversee the IT data analytics and information security of DSRIP data received from the New York State Department of Health (NYSDOH). SCC and SBMIT have engaged Cerner Corporation, a technology solutions vendor, as a Business Associate to provide a secure hosted and cloud-based IT Infrastructure environment. This Information Security Plan (ISP) is designed to protect SCC information assets and critical resources from internal and external threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. Information Technology (IT) security is achieved by implementing an appropriate set of controls; including policies, processes, procedures, organizational structures and various software and hardware functionality. The controls need to be established, implemented, monitored, reviewed and revised as necessary on an ongoing basis to ensure the security of SCC information assets.

The ISP governs the privacy, security and confidentiality of SCC data including but not limited to Protected Health Information, financial information, patient accounting information, sensitive information, regulated information, Human Resource information and public information. It is the responsibility of each SCC PPS Partner, PPS Associate, workforce member, agent, vendor and representative to protect SCC data appropriately. IT security measures are implemented to protect SCC information assets and ensure the confidentiality, integrity and availability of SCC data. Inappropriate use, access and or disclosure of SCC data, systems and applications exposes the data to risks such as virus attacks, network compromise affecting our systems and services, data loss and legal/regulatory ramifications.

All users on the SCC network are required to follow SCC Compliance Commitment Policy and are bound by this ISP as well as other SCC policies as a condition of their employment. All workforce members share responsibility for the security of the information and resources in their respective departments.

Purpose

The purpose of this ISP is to ensure the confidentiality, integrity and availability of data; to define, develop and document the information policies and procedures that support SCC goals and objectives; and to allow SCC to satisfy its legal and ethical responsibilities with regard to its IT resources.
Information security policies and procedures represent the foundation for the SCC ISP. Information security policies are guidelines for the appropriate use, management and implementation of information security practices throughout SCC.

Internal controls provide a system of checks and balances intended to identify improper use, access or disclosure of SCC data. Information assets are protected only when the information security policies are applied consistently.

This plan reflects SCC’s commitment to protecting our information/data assets, safeguarding the continuity of our business and fulfilling our legal obligations. This plan is reviewed annually or as necessary to address changes to our operations, systems and enterprise.

Scope

The SCC ISP applies to the SCC’s workforce members (refer to definitions), Business Associates and PPS Associates with access to SCC information assets including but not limited to data, images, text, hardware, software, systems applications, paper or other storage media/materials.

Definitions

Access: A user’s authorized ability to view, update, edit, and create orders, etc. to electronic Protected Health Information (e-PHI) based the user’s role and at a level necessary/required to perform their assigned duties.

Access Control: The process of controlling access to systems, networks and information based on business and security requirements.

Availability: The status of data or information in a format that is readily accessible and useable upon demand by an authorized person.

Breach: An unauthorized acquisition or disclosure of computerized data containing private, confidential or protected health information (e.g., social security number, driver’s license number or non-driver identification card number or account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account) or any form of protected health information.

Business Associate: A person or entity who creates, receives, maintains or transmits SCC PHI in the performance of a function or activity on behalf of SCC under a Business Associate Agreement.

Computer Workstation: An electronic computing device such as a laptop, desktop, tablet, PC, MAC/iOS, PDA or any other device that performs similar functions.
Confidentiality: A quality of protected access to data or information such that the data or information is not made available or disclosed to unauthorized persons or processes.

Control Activity: Policies, procedures, techniques and mechanisms to ensure the implementation of management’s response to reduce risks identified by a risk analysis.

DSRIP: Delivery System Reform Incentive Payment Program of New York State.

Encryption: The process of converting information into a secret code or scramble so that it is unreadable/unrecognizable except by someone with the decryption key to the code.

e-PHI: Any information, defined as protected health information, which is contained, maintained, transmitted, stored, used, disclosed or shared in electronic format/media.

Firewall: An electronic networking device that restricts access from one network to another network. A firewall supports and enforces an organization’s security policy for network access.

FTP: File transport protocol, a communications protocol governing the transfer of files from one computer to another over a network.

IDS: Intrusion Detection System software employed to monitor and detect possible attacks and behaviors that deviate from the normal and expected activity.

Information Assets: Defined data elements in any form, recorded or stored in any media, recognized as essential and valuable to the operations of the enterprise.

Information System: An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications and people.

Integrity: A quality of data or information that has not been altered or destroyed in an unauthorized manner.

IPS: Intrusion Prevention System. A device or application that identifies malicious activity, logs information about the activity, attempts to block/stop the activity and reports the activity.


IT: Information Technology

Medical Devices: As defined and listed in the Food and Drug Administration regulations, any instrument, machine, or implant, including accessories which are intended for use in the diagnosis or treatment of patients. Medical devices are not limited to electronic items and include consumables and accessories.
Network Infrastructure: The physical hardware used to transmit data electronically such as routers, switches, gateways, bridges, and hubs.

NIST: National Institute of Standards and Technology. A non-regulatory U.S. federal agency promoting innovation and industrial competitiveness by advancing measurement science, standards and technology to enhance economic security and improve quality of life.

Operational Information: Information generated or used in administrative, financial, legal, regulatory and quality improvement activities that are necessary for an organization to conduct healthcare-related business activities and support the core functions of treatment and payment. These activities include but are not limited to: quality assessment, quality improvement and patient safety activities, population-based activities to improve health care or reduce costs, protocol development, case management, care coordination, contacting providers or patients with information about treatment alternatives or options, reviewing competence, performance or qualifications of health care professionals including but not limited to potential misconduct, reviewing performance of health plans, conducting training programs for employees or non-health care professionals, accreditation, certification, licensing or credentialing activities, fraud and abuse detection and compliance monitoring, conducting medical review, legal counsel services, to meet regulatory requirements, auditing activities, business planning and development, business management, general administrative activities (creating de-identified health information or a limited data set, fundraising, some marketing activities, customer service and internal grievance resolution).

PPS: Performing Provider System in the DSRIP Program; a network of eligible providers collaborating to perform DSRIP projects, with a designated lead provider.

PPS Associate: Any individual or entity that participates in or does business with Suffolk PPS, including but not limited to (i) SCC and its employees, independent contractors, vendors, agents, suppliers, executives and governing body members; and (ii) all participating partner organizations and their employees, independent contractors, vendors, agents, suppliers, executives and governing body members.

PPS Partner: Individual or entity participating in the PPS.

Protected Health Information: Any information, including but not limited to, specimens, radiographs, photographs, any portion of the paper or electronic medical record or research data that contains patient identifiers; such as name, medical record number, social security number, date of birth, encounter number, test results, diagnoses, dates when services were provided, dates of admission, dates of discharge, date of death, etc., that relates to the past, present or future physical or mental health condition of an individual, the provision of health care to an individual, or payment for the provision of health care to an individual. This definition applies to information that is spoken, written or electronic in form and either directly identifies the individual or could reasonably be used to identify the individual. Any form of information that can identify an individual who has received, is receiving or will be receiving health care.
**Risk Analysis:** A process to determine which information resources/assets exist in an environment and require protection and to document potential risks from IT security failures that could cause loss of information confidentiality, integrity or availability.

**Security incident:** The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

**SMTP:** Simple Mail Transfer Protocol is used to transfer electronic mail between computers, over a network.

**Storage Media:** Any devices used to store electronic data including but not limited to usb-drives, CDs, DVDs, portable hard-drives, magnetic tapes, etc.

**Threat:** something or someone that can intentionally or accidentally exploit a vulnerability.

**Un-Protected Health Information:** Any form of PHI that is not rendered unusable, unreadable or indecipherable to unauthorized persons through a technology (encryption) or methodology (destruction).

**VPN/VDI:** Virtual Private Network/Virtual Desktop Infrastructure. A network/infrastructure that extends a private network across a public network (Internet), enabling users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network, and thus are benefiting from the functionality, security and management policies of the private network.

**Vulnerability:** a flaw or weakness in a system security procedure, design, implementation or internal controls that can be exploited by a threat and result in misuse or abuse of e-PHI or other confidential or business-related information/data.

**Workforce Member:** Any employee, volunteer, trainee, PPS Associate, or other individual affiliated with SCC whose work is under the direct control of SCC regardless of whether they are paid by SCC.

**IT Governance Commitments and Responsibilities**

IT governance is the responsibility of the SCC Board of Directors, SCC Executive Management and SBMIT. The governance consists of the leadership, organizational structures and processes to ensure that SCC IT sustains and advances SCC’s strategies, goals and objectives.

Executive Management has established the SCC Information Security Task Force to provide strategic direction and recommendations to ensure objectives and goals are achieved, determine risk and mitigate/manage risk adequately and utilize resources responsibly.
The SCC Information Security Task Force is charged with developing and implementing sufficient internal controls; providing ongoing training, promotion and awareness of IT security requirements and plans; and meeting customer needs within the appropriate legal framework.

**SCC Policy Statement**

Each PPS Partner and Business Associate is responsible to protect SCC resources by implementing, at a minimum, the security standards and procedures developed and approved by the SCC Board of Directors. All PPS Partners and Business Associates are required to meet the minimum standards. Departments are encouraged to adopt standards that exceed minimum requirements as appropriate for the protection of the Information Assets created, received, maintained and transmitted exclusively within the Department. Individuals within each department are responsible to comply with the security standards and policies developed and approved by SCC Board of Directors, to ensure the security of SCC Information Assets.

**Enforcement**

All individuals accessing SCC data are required to comply with federal and state laws and SCC policies and procedures regarding the security of SCC Information Assets. Any SCC employee, vendor or volunteer with access to SCC data who engages in unauthorized use, access, disclosure, alteration or destruction of SCC data is in violation of this ISP is subject to appropriate discipline, in accordance with collective bargaining agreements when applicable, up to and including termination; as well as possible civil and/or criminal penalties. Any PPS Associate who engages in unauthorized use, access, disclosure, alteration or destruction of SCC data in violation of this ISP is subject to appropriate corrective action, which may include exclusion from SCC, the DSRIP program and/or termination of a contractual relationship with SCC.

**Information Security Program**

Through this document and associated policies, SCC has established, documented and implemented an information security program. This program is designed to improve the effectiveness of IT operations and the ability to satisfy regulatory requirements. The program has been implemented to ensure the confidentiality, integrity and availability of SCC Information Assets while maintaining appropriate levels of accessibility. In order to ensure the security and confidentiality of SCC Information Assets and to protect against any known or potential threats to the security or integrity of the data, SCC has implemented all reasonable safeguards to keep our information and facilities secure. SCC has defined its own security controls, which are equal to or greater than security requirements and controls required by law and/or industry standards (ISO, NIST).
Risk Assessment

A risk assessment is a process which determines what information resources exist that require protection and to understand and document potential risks from IT security failures that cause loss of information confidentiality, integrity or availability. The purpose of a risk assessment is to help management create appropriate strategies and controls for stewardship of information assets. Because economics, regulatory and operating conditions continue to change, mechanisms are needed to identify and deal with the special risks associated with change.

Objectives are established before administrators can identify and take necessary steps to manage risk. Operational objectives relate to effectiveness and efficiency of the operations including performance, financial goals and safeguarding resources against loss. Financial reporting objectives pertain to the preparation of reliable published financial statements including prevention of fraudulent financial reporting. Compliance objectives pertain to laws and regulations which establish minimum standards of behavior.

SCC conducts a periodic risk assessment and/or business impact analysis in order to:

- Inventory and determine the nature of SCC information resources
- Understand and document the risks in the event of failures that cause loss of confidentiality, integrity and availability of information resources
- Identify the level of security necessary for the protection of the information resources

Control Activities

Control activities are the actions taken to minimize risk, for example; policies, processes, procedures, techniques, and mechanisms implemented to ensure management’s response to reduce risks identified during the risk assessment process are supported. When the assessment identifies a significant risk to the achievement of an objective, a corresponding control activity or activities is determined and implemented.

Control activities include a wide range of activities including approval, authorization, verification, reconciliation, review of operating performance, security of assets and segregation of duties. Control activities usually involve two elements: a policy establishing and defining the procedures to implement and the procedures/processes to implement the policy.

All policies are implemented consistently and are not in conflict with implementation of another policy or procedure/process.

Internal Controls

Effective internal controls are designed to provide reasonable assurance that organizational goals and objectives are met. Internal controls, procedures and processes also ensure that:

- Risks are reduced to an acceptable level
- Assets are safeguarded against waste, fraud, loss, unauthorized use or disclosure and misappropriation
• Processes are efficiently and effectively implemented in accordance with applicable laws and SCC policies. Controls are selected based on the cost of implementation relative to the reduction of risk to the organization. Non-monetary factors, such as reputation, resources, etc. are also considered. Adequate controls to mitigate risk need to be in place. These controls can be preventive, detective or corrective:

**Preventive Controls**

Preventive controls are designed to discourage or preempt errors or irregularities from occurring. They are the most cost effective control and include such processes as: credit checks, position descriptions, required authorized signatures, data entry checks and physical controls over assets to prevent their improper use (system access controls for example).

**Detective Controls**

Detective controls are designed to search for and identify errors after they have occurred. They are more expensive and usually require resources to implement. They measure the effectiveness of preventive controls and are the only way to effectively control certain types of errors. Account reviews and reconciliations, observations, periodic physical inventory, audits and internal auditors are examples of detective controls.

**Corrective Controls**

Corrective controls are designed to prevent the recurrence of errors. They begin when improper outcomes occur and are detected and keep the focus on the problem until the problem can be solved or the defect corrected. Quality teams and budget variance reports are examples of corrective controls.

**Control Environment**

The control environment, as established by the SCC Leadership, sets the tone for the organization and influences the workforce members’ level of compliance. Leaders of each Department establish a local control environment that is the foundation for all other components of internal control, providing structure and discipline.

Managers and employees are expected to have personal and professional integrity, achieve and maintain a level of competence that allows them to accomplish their assigned duties and understand the significance of developing and implementing adequate internal controls.

This requires managers and their staff to maintain and demonstrate at all times:
• Personal and professional integrity and ethical values
• A level of skill necessary to ensure effective performance
• An understanding of information security and internal controls sufficient to perform their assigned duties and responsibilities.
Managers and supervisors are also responsible for ensuring their employees are aware of the relevance and importance of their activities and how they contribute to the success of the control environment and the organization overall.

**Stony Brook Medicine Information Security Policy**

The SBMIT resources at SCC support the clinical, administrative, financial, educational and research activities of the enterprise and the use of these resources is a privilege that is extended to workforce members to facilitate their ability to achieve their duties and responsibilities. Any workforce member using the SCC network for any reason are required to adhere to strict guidelines regarding its use. Workforce members are being entrusted with the security of SCC information assets. Our security policy for information and other IT assets requires participation from each workforce member, at all times.

Any workforce member who uses or provides information resources has a responsibility to maintain and safeguard these assets. Each workforce member is expected to use the shared IT and information resources respectfully and with consideration for others.

Individuals are also expected to be informed and responsible for protecting their own information resources in any environment, shared or stand alone. It is unacceptable for anyone to use information resources for personal gain, to harm someone else, to violate law or SCC policy or perform unethical clinical, academic, research or business acts.

SCC’s *Security of Information Technology Resources* policy contains the standards for effective security requirements to ensure efficient use of SCC communication and information resources. The Chief Information Privacy and Security Officer, in cooperation/collaboration with various PPS Partners, Business Associates and subject matter experts, develop a training program(s) to ensure appropriate use by all workforce members with access to information assets.

**Organization of Information Security**

SCC ensures each PPS Partner and Business Associate implements a coordinated approach to protecting the information resources and assets under its custody by establishing appropriate and reasonable administrative, physical and technical safeguards that include all departments, individuals (workforce members) or others involved in the administration, installation, maintenance or use of SCC computing resources and information assets.

PPS Partner senior leaders are responsible to ensure the necessary resources are effectively applied to develop the capabilities needed to accomplish the enterprise mission. They need to assess and incorporate the results of the risk analysis/assessment activities into the decision making process.
The SBMIT Chief Information Officer (CIO) is responsible for the overall data gatekeeper, technology planning, budgeting and performance including the information security components. Decisions regarding information security are based on an effective risk management program.

The SBMIT Chief Information Privacy and Security Officer (CIPSO) is responsible for the SCC’s information privacy and security program. The program consists of policy and procedure creation, implementation, review and update; workforce awareness, training and communication; compliance auditing/monitoring activities, risk analysis/assessment and risk management; investigations of incidents and allegations, mitigation, reporting and discipline. The CIPSO has a leading role in implementing an appropriate structured methodology to facilitate identification, evaluation and mitigation of risk to IT information systems and assets.

Data Owners are responsible for ensuring proper controls are in place to address the confidentiality, integrity and availability of the IT system(s) and data they own.

SBMIT leadership take an active role in the IT security process (Networking, Sys Admin, application owners, database administrators, Client Support and HelpDesk). The leaders involved in IT procurement decisions are responsible to ensure appropriate safeguards are in place to address the confidentiality, integrity and availability of information assets at all times.

IT Security Leaders for each PPS Partner and Business Associate are responsible for proper implementation of security requirements in the IT systems upon startup and as changes occur.

Identity and Account Management is responsible to ensure access to information assets, data, applications and/or systems is granted to only those who require access to perform their job responsibilities. PPS Partner leads are responsible for the identity management and authentication of their users.

Data User is an individual workforce member who has been granted authorization to access information/data. The user uses the data only for purposes specified in their position description or as assigned by their supervisor/manager and complies with security measures specified in SCC Information Privacy and Security policies, procedures and processes.

**Accountability for Assets**

Proper internal control is maintained over all IT assets at all times. Proper IT asset management from requisition to disposal ensures adequate safeguards of the IT assets.

PPS Partner Leads assist in the identification of those workforce members with access to PHI/e-PHI and SCC/SBMIT Infrastructure maintains an inventory of IT assets. Individuals authorized to access SBMIT assets (information, data, applications and/or systems) adhere to appropriate roles and responsibilities when utilizing the assets.
**Information Classification**

Information classification is necessary to determine the sensitivity and criticality of information assets, which provides a basis for protection and security efforts and access control. The classification of information can be derived from federal and state laws that govern the privacy and confidentiality of data. For example, HIPAA protects identifiable health information, CFR 42 part 2 protects the confidentiality of Alcohol and Substances Abuse treatment information, CFR 45 part 46 protects human subjects research data, NYS PHL Article 27-F protects the confidentiality of HIV/AIDS related information, NYS MHL protects the confidentiality of mental health information and GINA (federal and state laws) protect the confidentiality of genetic information.

Information classification applies to all data (clinical, research, financial, employee and patient data) collected in any form electronic or hard copy that is created, received, maintained and/or transmitted except where a different standard is required by grant, contract or law.

SCC data is classified into one of three following sensitivity categories/classifications; Confidential, Internal/Private or Public. Although all data requires some level of protection, certain data are considered more sensitive which correspondingly requires increased security and controls. Access to HIV, mental health, alcohol and substances abuse treatment and other sensitive data is restricted based on role and access level. A warning notification is displayed when accessing such patient information indicating the following:

*The information contained in this record is being protected from inappropriate/unauthorized access. All access activity will be logged and audited. You may access this record for treatment/clinical or payment/billing purposes or other health care activity only.*

Data is reviewed on a periodic basis to determine the appropriated classification according to the use, sensitivity and importance of the data to the enterprise and in compliance with federal and/or state laws.

The level of security required for each classification depends largely on the effect unauthorized access and/or disclosure of the information would have on the operations, finances and reputation of SCC and/or the privacy of SCC’s customers (NYS DOH, patients, employees, contractors/vendors, etc.)

Confidential information – the unauthorized access/disclosure, acquisition, compromise, or destruction of such data would result in severe damage to the enterprise and/or its customers. This can be patient, subject or employee information such as social security number, date of birth, credit card, bank account information, medical records, identifiable patient information/PHI/e-PHI and/or information protected under quality/legal privilege, federal or state law). The use of this data is limited to SCC business only and access to this information is restricted to only those with a “need to know”. This data may be marked confidential, attorney-client privileged, confidential and required to be collected and maintained pursuant to Public Health Law Sections 2805-j,k,l and m, and Education Law Section 6527, etc., as applicable.
1) Internal/Private – internal use information for business operations that is not confidential but requires guarding due to proprietary, ethical or privacy considerations, although not specifically protected by statute, regulation or other legal obligations or mandates. Unauthorized use, access/disclosure, acquisition, modification, loss or deletion of information at this level could cause financial loss, damage to SCC reputation or violate an individual’s right to privacy; for example, employee information. This information is intended for internal/business use only by workforce members with associated duties and responsibilities.

2) Public – information that is not publically disseminated, but is accessible/available to the general public. This data is either explicitly defined as public information (state employee salaries), intended to be readily available to individuals (patient directory – unless the patient has opted out, employee work email address, etc.), or is not specifically classified as confidential or internal/private. Knowledge of this information does not necessarily expose SCC to financial or reputational loss or place SCC’s information assets at risk. Publically available information is subject to appropriate review or disclosures procedures to mitigate potential risks of inappropriate disclosure of data (such as SCC Board of Directors/Executive Leadership review of SCC offerings for posting in local media or review of position postings).

Identity and Access Management

Identity and access management ensures accurate identification of authorized workforce members and provides secure authenticated access to and use of network services. Identity and access management is based on a set of principles and control objectives to:

- Ensure unique identification of each workforce member and assignment of access privileges
- Allow access to information resources only by authorized individuals
- Limit concurrent sessions to one session
- Manage inactivity to restrict unauthorized access and require the user to re-authenticate through session lock-out(s)
- Ensure periodic review of workforce membership and review of their authorized access rights
- Maintain effective access mechanisms through evolving technologies
- Periodic audit of access activities to include review of audit logs.

Access control refers to the process of controlling access to systems, networks and information assets based on business and security requirements. The goal is to prevent unauthorized access, use and disclosure of SBM information assets. Access control measures include secure and accountable means of identification, authentication and authorization.
Identification

Identification is the process of uniquely naming or assigning an identifier to every individual or system to enable decisions about the levels of access that are granted. The significance of an identity process is that each user requiring access for their roles and responsibilities is uniquely identifiable from all other users.

Authentication

The authentication process determines whether someone is, in fact, who they declare to be. Authentication validates the identity of the individual. Authentication factors can be something you know (password), something you have (token), or something you are (biometric). Two factor authentication consists of two of the three factors, (i.e. password and token) in these distinct categories. For the purpose of access control, authentication verifies one’s identity through IT.

Passwords are a significant aspect of computer security. They are the frontline of protection for user accounts both for SCC information asset and the user. A poorly chosen password can result in compromise of the entire SCC network. Adhering to secure password procedures assists in reducing compromised user accounts. All users who are granted access to SCC network, systems and applications are responsible for selecting and securing their passwords. Users are held accountable for all activity performed with their access (log-on/sign-on).

Authorization

Authorization is the process used to grant permissions to authenticated users. Authorization grants the user the right to use the information assets and determines what type of access is permitted (read-only, read/write, etc.)

These access rights to information assets is determined by PPS Partner leads. The authorization rules are applied and enforced consistently among the PPS Partners. The level of access depends upon the roles and responsibilities of the user. The level of control depends upon the classification of data and the level of risk associated with the loss or compromise of the information.

Criteria is established for account eligibility, creation, maintenance and expiration/termination. Access to Confidential information is authorized by well-established processes approved by SCC Board of Directors, Executive Leadership and based on a user’s roles and responsibilities.

Depending on the relative sensitivity of the data/information, access is restricted to HIV/AIDS and mental health care provided through New York State Office of Mental Hygiene certified locations/facilities to only healthcare providers and those users assigned to work in the restricted locations/facilities respectively.
SCC PPS Partner leads and data owners periodically review user privileges and submit requests to SCC Information Security Task Force for modification or inactivation of accounts when access is no longer required.

All workforce members are required to sign and date the SCC “Workforce and Electronic Information Access Confidentiality Acknowledgement Statement” upon hire and annually thereafter. All contractors/vendors requiring access are required to sign and date the confidentiality statement included on the account request submission.

Inactivity time-outs are implemented for workstations that are available in clinical areas (nursing units, ambulatory/outpatient clinical locations) and for all workstations and portable devices (laptops, smartphones) for all systems/applications containing information assets. The period of inactivity varies depending upon the location and accessibility of the workstation or device to ensure those easily accessible time-out no longer than 10 minutes and those located in closed limited access locations (operating room) time out is extended to ensure patient safety.

Audit trails exist to detect and respond to system penetration, infection of systems and data due to malicious code, catastrophic system loss, compromise of data integrity, unauthorized access to information and as required by law.

Procedures are documented for the timely revocation of access privileges and return of SCC owned assets (keys, ID badges, laptops, smartphones, and tokens) and return or certification of destruction of information/data for terminated workforce members and contractors/vendors.

Remote Access

Remote access to information technology resources (switches, routers, computers, etc.) and to sensitive or confidential information (social security numbers, credit card numbers, PHI, etc.) are only permitted through secure, authenticated and centrally managed access methods such as VPN, VDI, SecureLink that provide encryption and secure authentication.

When accessing sensitive or confidential information remotely users are prohibited from accessing such information in an unsecure location (where over-the-shoulder viewing or access by unauthorized individuals is possible) or storing such data on local drives (personal computers, laptops, CD, smartphones, usb-drives, etc.). External computers used to access SCC resources or sensitive/confidential information must be secure. This includes patching, (operating systems and applications), possessing updated anti-virus software, accessing through a secure process (VDI, VPN, etc.) in order to operate within the security of the SCC/SBMIT firewall and being configured in accordance with all relevant SCC/SBMIT policies and procedures.

Privileged Access

Systems administrators routinely require access to information resources to perform essential system administrative functions critical to the continued operation of SCC. Such privileged access often referred to as “administrator access” is enabled to perform system administrative functions only to limited users responsible for the continued operation of the system/application.
The number of privileged accounts are kept to a minimum and only provided to those workforce members whose roles and responsibilities require it. Administrators or users who require privileged accounts also have non-privileged accounts to use when performing daily routine access and do not use their privileged account for non-authorized purposes. Activities performed using a privileged account is logged and the logs are reviewed periodically by an independent and knowledgeable SCC/SBMIT leader.

Workforce members who manage, operate and support SCC information systems, including individuals who manage their own systems are expected to use appropriate practices in providing for the security of the systems they manage. Responsibility for systems and application security is assigned to individual(s) knowledgeable about the technology used in the system and in providing security for the technology.

Segregation of Duties

Tasks involved in critical business processes are performed by separate individuals. Responsibilities of programmers, systems administrators and database managers do not overlap, unless authorized by the data owner or SCC leadership. Duties and responsibilities are assigned systematically to a number of individuals to ensure that effective checks and balances exist. Such controls keep a single individual from subverting a critical process. Key duties include authorizing, approving and recording transactions; issuing and receiving assets; and reviewing and auditing transactions.

Segregation of duties are maintained between the following functions:
  Data Entry
  Computer Operation
  Network Management
  Systems Administration
  System Development and Maintenance
  Change Management
  Security Administration
  Security Audit

Qualified and continuous supervision is provided to ensure that internal control goals are achieved. PPS Partner leads continuously review and approve the assigned work of their staff and provide necessary guidance and training to ensure errors, waste and wrongful acts are minimized and management directives are completed.

Access Audits/Access Logs/Access Reports

All systems access is logged and recorded in compliance with federal guidelines to include but not limited to the following auditable events:

Server alerts and error messages; user log-on and log-off (successful and unsuccessful); system administration activities; modification of privileges and access; policy changes;
privilege functions; process tracking; system events; administrator activity; authentication checks; authorization checks; data deletions; data access; data changes; permission changes; start-up and shut down; application modifications; application alerts and error messages; configuration changes; account creation, modification or deletion; file creation and deletion; read access to sensitive information; modification to sensitive information; printing of sensitive information; all successful and unsuccessful authorization attempts; enabling and disabling of audit report generation services; command line changes, batch file changes and queries made to the system.

The date/time stamp is recorded in GMT and is accurate within thirty (30) seconds. The system is set-up to compare the internal clock at least daily and upon system boot against NIST Internet Time Servers (http://tf.nist.gov/tf-cgi/servers.cgi) as the authoritative time source and synchronize the internal clock to the authoritative time source with the time difference is greater than thirty (30) seconds.

The audit tool reporting responsibilities are assigned to limited individuals who do not have any other access or responsibilities associated with the system. The audit information and tool are protected from unauthorized access, modification and deletion. Audit logs are stored in accordance with applicable Retention Schedules with sufficient storage capabilities to ensure data loss/overwrite is prohibited. The audit logs are backed up weekly onto a physically different system or system component than audited component. Audit logs are reviewed periodically for unusual, unauthorized and/or inappropriate access and findings are reported to the SCC Information Privacy and Security Officer for investigation and appropriate corrective/disciplinary processes.

**Communication and Operations Management**

System communications protection refers to the key elements used to assure data and systems are available and exhibit the confidentiality and integrity expected by SCC and SBMIT. The appropriate level of security applied to the information and systems is based on the classification and criticality of the information and the business processes that use the information. System’s integrity controls protect data against improper alteration and destruction during processing, storage and transmission over electronic communication networks.

The key elements of system and communications protection are backup protection, denial of service protection, boundary protection, use of encryption, public access protection and protection from malicious code.

Operations management refers to implementing appropriate controls and protections on hardware, software and resources; maintaining appropriate auditing and monitoring; and evaluating system threats and vulnerabilities. Proper operations management safeguards all of SCC/SBMIT’s computing resources from loss or compromise including stored media, communication hardware and software, processing equipment, standalone computers and printers.
Network Security

Network attacks launched from the Internet or from SCC PPS Partner or Business Associate networks can cause significant damage and harm to information resources and assets including unauthorized access to and/or disclosure of confidential information. In order to defend against attacks, firewall and network filtering is applied in a structured and consistent manner.

SCC Business Associates and SBMIT maintain appropriate configuration standards and network security controls to safeguard information resource from internal and external network threats. Firewalls and Intrusion Detection Systems (IDS) are implemented for the SCC Business Associate networks and SBMIT clinical and non-clinical networks and Intrusion Prevention Systems (IPS) are deployed on core services to prevent denial of service attacks, malicious code or other traffic that threatens systems within the network.

Security Monitoring

Security Monitoring provides a mechanism to confirm that information resource security controls are in place, effective and not being bypassed. Early identification of wrongdoing and security vulnerabilities are the primary goals of security monitoring. Early detection can prevent possible attacks and/or minimize their impact on SCC information systems.

Any equipment attached to SCC PPS Partners environment or the Cerner Works environment are subject to security vulnerability scans. The goal of the scanning is to prevent/reduce the vulnerability of SCC information systems/network to hacking, denial of service attacks, infection and other security risks arising from internal and external sources. SCC PPS Partners environment and the Cerner Works environment are scanned using commercial and open source software to monitor and assess the security of the network. Servers storing confidential/critical information are given a higher priority but other servers are scanned as well. Additionally, the SBMIT Information Security Task Force receive notification from external sources including but not limited to HANYS, GNYHA, HIMSS/CHIME, OCR SUNY IT Security, FBI Liaison Alert System (FLASH) and FBI Health Sector Cyber-Security/Crime Division. The task force reviews all alerts, advisories, directives and notifications promptly, prepares and disseminates a message as necessary to appropriate personnel including but not limited to the SBM Leadership, SBM General Counsel, SBMIT Leadership and the workforce when applicable. The SBMIT leadership implement when applicable security directives promptly in accordance with time frames indicated in the directive to ensure ongoing compliance.

Encryption

SCC PPS Partners, SCC Business Associates and SBMIT have implemented standards for encryption to ensure sensitive/confidential data is protected at rest and during transmission. Remote hosted information assets are protected by the vendor while the data is at rest and secure dedicated encrypted (lines) are used for the transmission of the data from the remote site into the SCC network. SCC/SBMIT owned laptops are distributed with hard disk encryption and/or locator/remote-wipe capability. Data/information assets are not stored on local equipment
(desktop or portable) unless the equipment/devices is encrypted. All sensitive/confidential and internal/private data are stored on either individual or limited access group secure network server shares. Encryption of information in storage presents risks to the availability of the information in terms of latency and loss of encryption key. Therefore, SCC/SBMIT data center security safeguards do not include encryption of data at rest for individual and group network shares.

**Virus Protection**

Viruses are a threat to SCC as infected computers can transmit confidential information to unauthorized third parties, provide a gateway for unauthorized access or use of the internal network, contaminate or infect other network connected devices or interfere/disrupt/terminate SCC PPS Partner, SCC Business Associate and SCC/SBMIT services. Antivirus software is provided by SCC/SBMIT for all SCC/SBMIT owned information technology equipment. SCC/SBMIT Network Services is responsible for creating and implementing procedures to ensure antivirus software is applied with the latest updates on all IT assets connected to the network.

SCC/SBMIT reserves the right to review any device attached to the SCC/SBMIT network (public or non-public) for adequate virus protection, to deny access to the network to any device found to be inadequately protected and disable network access to any device that is not sufficiently protected or noted to be infected with a virus. Once the device has been cleaned, updated with current antivirus software and operating system and application patches installed network access can be re-established.

**Backup and Recovery**

All electronic information either remote hosted with vendor provided appropriate backup and recovery processes by contract, or stored on secure servers in SCC PPS Partner, SCC Business Associate and/or SCC/SBMIT data center with nightly backup for the purpose of disaster recovery and business continuity. For critical data a mirror system is implemented to facilitate rapid recovery. SCC/SBMIT Network Services is responsible for the creating and implementing minimally appropriate backup and recovery processes and procedures as follows:

- All data and utility files are adequately and systematically backed up including all patches, fixes and updates
- Records of what is backed up and to where is maintained.
- Records of software licensing is backed up
- Backup media is precisely labeled containing the following:
  - System Name
  - Creation Date
  - Sensitivity Classification
  - Record Retention in accordance with applicable federal and state Record Retention laws.
Copies of backup media together with the backup record are stored in secure limited access location(s) at a sufficient distance away to avoid damage from a disaster at the main site. Periodic tests of data/software restoration from the backed up copies is undertaken to ensure the copied data can be relied upon for use in the case of an emergency.

**Systems and Application Security**

It is essential that applications are developed properly to ensure data is processed in a manner that protects the integrity of the data. Appropriate application software maintenance includes documented change control and prevents malicious code or virus attack.

**System Development and Maintenance**

All stages of an information system life cycle requires security considerations to ensure conformance with applicable security regulations/requirements, protect sensitive/confidential information through the information life cycle, facilitate efficient implementation of security controls, prevent introduction of new risks when the system is modified and ensure proper removal of data when the system is retired/replaced.

To ensure system security is considered during the development and maintenance stages SCC adheres to the following minimum requirements during each phase:

- **Feasibility Phase** – high level review to ensure security requirements can support business case
- **Requirements Phase** – define any initial security requirements or controls to support business requirements
- **Design Phase** – verify appropriate security controls for the baseline have been identified and ensure change control is established and user for the remainder of the life cycle. Repeat verification with each design change or as warranted
- **Development Phase** – verify and validate all security controls identified form design phase. Repeated throughout as changes are made or as warranted
- **Implementation Phase** – final verification of existing controls and appropriate levels of risk mitigation

**Change Control**

Change control is the process that management uses to identity, document and authorize changes to an IT environment. An effective change control process minimizes disruptions, unauthorized alterations and errors that can occur as a result of implementing change(s). To develop appropriate and effective change control procedures; design consideration such as environment complexity and size are necessary. For example, complex applications maintained by large IT staff or those that represent high risk require more formalized and extensive processes than
simple single person managed applications. In all cases clear identification of who is responsible for the change control process is necessary.

The change management process consists of:

- **Change Request Initiation and Control** – Requests are changes to be standardized and subject to management review. Changes are categorized and prioritized and specific procedures are in place to handle urgent matters. Change requestors are kept informed about the status of their request.

- **Impact Assessment** – A procedure is in place to ensure all requests for change are assessed in a structured format to confirm all possible impacts on the operational system and its functionality are addressed.

- **Control and Documentation of Changes** – Changes to production systems are made only by authorized individuals in a controlled manner. Where possible a process for rolling back to the previous version is identified. It is also important to document what changes have been made. At a minimum a change log is maintained that includes:
  - A Brief functional description of the change
  - Date the change was implemented
  - Who made the change
  - Who authorized the change
  - What technical elements were affected by the change (program modules, database tables/fields, screens and forms, etc.)

- **Documentation and Procedures** – The change process includes provisions that whenever system changes are implemented, the associated documentation and procedures are updated accordingly.

- **Authorized Maintenance** – Staff maintaining systems are to have specific assignments and their work monitored as required. In addition, their system access rights are controlled to avoid risks of unauthorized access to production environment.

- **Testing and User Signoff** – Software is thoroughly tested, not only for the change itself but also for impact on elements not modified. A standard suite of tests is developed in addition to a separate test environment. The standard test suite is designed to identify if core elements of an application were inadvertently affected. Data owners of the systems are responsible for signing off and approving proposed change(s).

- **Testing Environment** – Ideally systems have at least three separate environments (development, testing and production). The test and production environments are as similar as possible, with the possible exception of size. When cost prohibits three separate environments then testing and development take place in the same environment; but
development activities need to be closely managed or discontinued during acceptance testing. Untested code or development is never to appear/occur in a production environment.

- Version Control – Control is placed on production source code to ensure only the latest version is being updated to avoid previous changes being inadvertently lost when a new change is moved into production. Version control is significant to effectively back out of a change that exhibits unexpected/negative effects.

- Emergency changes – Emergency situations occur that require(s) program change controls to be overridden. For example, permitting programmers access to production. However, at least a verbal authorization is obtained and the change documented as soon as possible.

- Distribution of Software – As a change is implemented it is important that all components of the change are installed in the correct locations and in a timely manner.

- Hardware and System Software Changes – Changes to hardware and system software are also tested and authorized before being applied to the production environment. These changes are documented in the change log.

If a vendor supplies patches, they are reviewed and assessed for applicability and potential impact to determine whether their fixes are required by the system.

**Physical Security Measures**

Physical security controls and secure areas are used to minimize unauthorized access, damage and interference with information and information systems. Physical security includes environmental safeguards to control physical access to IT network, IT equipment, output devices including but not limited to printers, copiers, scanners, faxes, etc. and data/information assets in order to protect these information technology resources from unauthorized use.

Access to areas containing confidential/sensitive information is physically restricted (data center, clinical areas, etc.). Access to all entry points into the data center are protected by electronic access control mechanisms to validate access and ensure only authorized individuals enter the facility. Video cameras and alarms at data center points of entry are monitored 24/7 by SBMIT HelpDesk staff. Cameras located inside the data center monitor activities of individuals granted access to the data center. An audit trail of all access is securely maintained in compliance with applicable Record Retention policy and guidelines.

All individuals with access to clinical areas and/or the data center are required to wear their appropriately issued SCC PPS Partner, SCC Business Associate or SCC/SBM identification (ID) badge on their outer garments so that both their picture and printed information (name, title and department) are clearly visible. ID badges are also used to monitor access to restricted clinical areas using electronic access control mechanisms to validate access by only authorized individuals.
All workforce members are encouraged to challenge unescorted people and those not wearing visible identification. Access rights to secure areas are regularly reviewed and updated as appropriate.

Upon workforce member termination or separation from SCC PPS Partner, SCC Business Associate or SCC/SBM service, access to restricted areas is revoked as well as disabling of network/systems/application access.

All output devices are located in limited staff only access areas, locked private offices or office suites located in non-public access areas and locked when unattended. The output devices include but are not limited to printers, copiers, scanners, faxes and any audio or other recording devices. The devices are routinely checked for output and any output is promptly removed from the devices and turned over to the appropriate intended recipient, when applicable.

Visitors

Visitors are properly identified with a current, valid form of identification (corporate ID, state issued driver’s license or non-drivers ID, U.S. passport or visa). At SBM a temporary facility badge allowing access to clinical area is obtained at the hospital main lobby information desk at the RepTrax monitor.

Physicians/students/vendors attending meetings/tours are arranged and sponsored by various clinical departments. At SBM a temporary ID badge is obtained at the SBM ID office located in the HSC Level 3 or through RepTrax, as appropriate. The meeting/tour visitor(s) is not permitted to walk throughout the facilities unaccompanied and the sponsoring department obtains a signed Visitor/Tour Participant Confidentiality Agreement to keep on file for each visitor.

Surveillance

There are several methods of surveillance throughout the facilities. Video-monitoring without recording capability for patient safety occurs in locations designed with signage. Video-recordings for safety and security in public access locations are overseen by SCC PPS Partner’s, SCC Business Associate’s and SBM Security. Video-recording for quality review purposes is overseen by the Continuous Quality Review team in the specific clinical setting using this technology.

Equipment Control

The assigned user of IT resources is considered the custodian for the resource. If/when the assigned resource(s) is damaged, lost, stolen or is otherwise unavailable for business purposes, the custodian promptly notifies the department manager/director. For damaged equipment a request/ticket is submitted for repair/replacement to the appropriate SCC PPS Partner, SCC
Business Associate or SCC/SBMIT HelpDesk. For lost/stolen IT resources prompt notification to SCC Information Security Task Force hipaa@stonybrookmedicine.edu is required.

IT resources are secured at all times to prevent physical tampering, damage, theft or unauthorized access.

An inventory of all IT resource assets (equipment and media) is maintained by SCC/SBMIT Infrastructure.

**Computer Data and Media Disposal**

Proper disposal of information assets is essential for controlling and securing confidential and sensitive data including but not limited to; patient information, human resource information, finance data, PHI and credit card information, etc. If information on systems/IT resources is not properly removed prior to disposal or surplus it can be accessed, used, disclosed by unauthorized individuals.

Media or devices containing confidential/sensitive or business related information is processed through the appropriate HelpDesk for tracking, review, approval and verification for each SCC PPS Partner, SCC Business Associate or SCC/SBMIT for the removal of data and/or destruction of the device/hard-drive.

SCC/SBMIT is committed to compliance with federal and state laws associated with the protection of confidential information and adheres to Software licensing agreements.

**Business Continuity**

SCC/SBMIT, SCC PPS Partners and SCC Business Associates provides a safe, secure IT environment to serve our customers’ needs in the performance of their roles and responsibilities and ensures the stability and continuity of business operations.

**Business Impact Analysis**

Data owners and Data Custodians perform appropriate business impact analyses that correlate specific system components with the criticality of the services the system provides. The analyses are documented and reviewed periodically for accuracy. Consequences of a disruption to the system components are identified and documented. Critical IT resources are identified through collaboration with users and those supporting the system to determine the full range of support provided by the system including security, administrative, technical and operational. Infrastructure requirements supporting the IT resource are included in the analysis such as electrical power, telecommunications connections and environmental controls. Specific IT equipment such as application and authentication servers are considered critical whereas printer/print servers do not necessarily support critical services.
Outage Impacts and Allowable Outage Times

Data owners and custodians analyze the critical resources identified in the Business Impact Analysis to determine the impact on IT operations if a resource were disrupted or damaged. The following evaluations are required:

- The effects of the outage over time enable SCC/SBMIT to identify the maximum allowable time that a resource can be unavailable before it prevents or inhibits performance of essential functions.

- The effects of the outage on related resources and dependent systems to assist in identifying any resulting effects that occur to other processes that rely on the disrupted system.

- The effects of the outage on revenue streams and costs expenditures to identify areas of financial concern that lead to a delay in recovery.

Recovery Priorities

Data owners and custodians develop recovery priorities for the system resources. A scale based on criticality is used to prioritize the resources (mission critical, business essential, business core, business supporting). Mission critical and business essential resources require minimal downtime and restoration within the allowable outage times; whereas business core and business supporting allow for restoration of operational capacity over a longer time frame.

Recovery strategies are based on the prioritization/criticality scale and implementation during contingency plan activation. SCC PPS Partners, SCC Business Associates and SCC/SBMIT are able to make informed, tailored decisions regarding contingency resource allocation and expenditures by prioritizing recovery of critical components.

Disaster Recovery

A disaster recovery plan is an ongoing process of planning, developing and implementing disaster recovery management processes and procedures to ensure efficient and effective return of critical functions in the event of an unscheduled interruption in service.

The components of the disaster recovery plan are clear, concise and easy to implement in an emergency. Documents such as checklists and step-by-step procedures are followed to ensure specific actions are followed for return to baseline. Detailed information is provided for continued business operations and performance of all required tasks while IT resources (hardware, network, data) are being recovered. The order in which systems are recovered at to what level of functionality is based upon the Business Impact Analysis. Not all systems need to be recovered at once or to 100% for the system to begin functioning.
Information Security Incident Response

A security incident is an actual or suspected violation of computer security policies, acceptable use policies or standard computer security practices. A security incident could result in unauthorized access, misuse and/or inappropriate disclosure of confidential information; place the functionality of SCC PPS Partner, SCC Business Associates and SCC/SBM IT infrastructure at risk and/or provide unauthorized access to SCC resources and/or information.

When such incidences occur SCC has a plan to which includes reporting, investigating and resolving/mitigating the incident to ensure the confidentiality, integrity and availability of SCC information assets. If a user suspects that information or information systems are being misused or are under attack (phishing attempts) the user is obligated to report the incident to the SCC Information Security Task Force hipaa@stonybrookmedicine.edu. Immediate action to isolate the incident from the network is essential to protect SBM information assets.

1) Contact the SCC Information Security Task Force, systems administrator or designated IT support if applicable
2) Your notification needs to contain; a description of the incident, any steps already taken to correct or isolate the problem; the names/titles of other IT professionals already contacted regarding the incident.
3) For computer problems provide the name and location of the computer
4) For email issues a copy of the email (phishing and spam) including to/from, subject and date.