NIGHTINGALE PREVENTATIVE CARE

HIPAA Security Policy
Job Description for Privacy & Security Officer

Reviewed / Revised: September 2014

General Purpose

The Combined Privacy and Security Officer oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to *Nightingale's* policies and procedures related to the security and privacy of access to, use and disclosure of patient health information in compliance with federal and state laws and this Organization's security and privacy practices.

Responsibilities

The HIPAA Privacy & Security Officer's duties include:

- Manage all HIPAA security and privacy related compliance activities.
- Development, implementation and maintenance of appropriate security and privacy related policies and procedures.
- Conduct Security Risk Assessments (SRA), and / or Privacy Risk Assessments (PRA) as needed or required.
- Ensure all physical, technical and administrative safeguards are in place and updated regularly.
- Ensure privacy and security related (HIPAA, maintenance, software update, etc) documentation retained for a minimum of 6 years (the HIPAA Rule mandatory timeframe).
- Investigate, document and mitigation for HIPAA security non-compliance events or incidents.
- Develop or obtain appropriate privacy and security awareness training for all workforce members, as appropriate.
- Administer the process for receiving, documenting, tracking, investigating, and taking action on all privacy or security complaints in conjunction with HR, other Compliance Officers and legal counsel.
- Cooperate with HHS and its Office for Civil Rights, other legal entities, and Organization officers in any privacy and / or security compliance reviews or investigations.
- Ensure Contractors are compliant with HIPAA and afford the highest levels of protections.
- Manage Accounting of Disclosures Log and processes, if needed.
- Serve as contact point for Covered Entity (CE) privacy questions, requests, investigations and other similar processes.
- Perform breach notification when appropriate.
- For Covered Entities; Ensure Business Associates and through them their Sub-

contractors are following all HIPAA, state and other Federal privacy and security rules. Evaluate BAs before and during intial Busineess Associate Agreement (BAA) negotiations and with on-going monitoring.

- For Business Associates; Ensure Sub-contractors are following all HIPAA, State and Federal privacy and security rules. Evaluate BAs before and during intial Sub-contractor agreement negotiations and with on-going monitoring.

Qualifications

- Knowledge and experience in information privacy and security rules, current regulations and laws; access; release of information; and release control technologies.
- Knowledge in and the ability to apply the principles of health information, project management, and change management.
- Demonstrated organization, facilitation, communication, and presentation skills.

NIGHTINGALE PREVENTATIVE CARE

HIPPA Security Policy

Documentation For Security and Privacy Compliance

A. Coverage

Nightingale (hereafter referred to as the 'Organization') workforce members that access, use, disclose confidential patient information.

Review / Revision Dates: September 2014

B. Purpose

The purpose of this policy is to provide guidance on development, management and maintenance of documentation related to HIPAA requests, complaints, investigations and on-going compliance activities.

C. Policy Statement

This policy is intended to govern the creation, use, and maintenance of documentation (documents) related to HIPAA compliance. Workforce members must document in writing (or electronic) all HIPAA-related activities that require documentation. Any action, activity or assessment that must be documented, shall be documented in accordance with this and other policies and procedures implemented by the Organization. And such documentation must be used, applied and reported according to other Organizational policies.

This Organization retains all HIPAA related documentation for a minimum of six (6) years from the date of its creation or modification, or the date when it was last in effect, whichever is later.

Documentation to be strongly considered for retention throughout the entire the defined HIPAA retention period includes, but is not limited to the following. All appropriate staff that needs access to this information must be provided such access.

- Security Risk Assessment (Analysis), also known as 'SRA'.
- Privacy Risk Assessment (PRA).
- Privacy and security risk management plan and program documentation.
- Business Associate Agreements (or if a BA, Sub-contractor agreements) , confidentiality agreements and other privacy or security compliance agreements or contracts.
- List of software used to manage and control internet access and use.
- Security issues logs.
- List of workstations, their use and employees that can access.
- Audit log copies.
- Privacy and security education and training.

NIGHTINGALE PREVENTATIVE CARE

Authorization to Access Electronic PHI

D. Coverage

Nightingale (hereafter referred to as the 'Organization') workforce members that access, use, disclose confidential, individually identifiable, electronic protected health information (PHI or ePHI).

E. Review / Revision Dates

September 2014

F. Purpose

The purpose of this policy is to provide guidance in relation to authorization to access electronic PHI and supervision of workforce members given this access.

G. Policy

All Organization workforce members, Business Associates and Contactors must comply with HIPAA regulations pertaining to the authorization and supervision of workforce members who will be accessing individually identifiable health information as part of their work-related duties, as delineated in § 164.308(a)(3). Authorization and supervision of appropriate access, use and disclosure of PHI assists in reducing overall Organizational risk, and reduce HIPAA violations and breaches.

The Organization only permits workforce members who have been appropriately authorized, to have access to PHI. These workforce members must be appropriately supervised. These workforce members shall have access to only to the minimum amount of PHI needed to perform their roles. All of these authorizations and supervision will be documented and retained for a minimum of the HIPAA mandatory retention period.

NIGHTINGALE PREVENTATIVE CARE

Workforce Security Clearance

H. Coverage

Nightingale (hereafter referred to as the 'Organization') workforce members that access, use, disclose confidential protected health information (PHI). Our workforce includes all clinical providers, clinical supportive staff involved in the care of patients, volunteers, students and other staff members involved in the routine operations of our delivery of care.

I. Review / Revision Dates

September 2014

J. Purpose

The purpose of this policy is to provide guidance in reference to security background checks and clearance as related to IT security.

K. Policy Statement

Screening and assigning specific access controls to IT systems containing PHI within the Organization's workforce can reduce the likelihood of HIPAA violations and breaches surrounding the access, use and disclosure of PHI. This Organization provides appropriate level of access to PHI to all members of the workforce. These access levels shall be based upon the nature of each workforce member's duties and responsibilities. Workforce members shall have access to the entire set of PHI that they need to do their jobs, but no more access than that. HIPAA Minimum Necessary principals will always apply. No member of the workforce shall have access to a higher level of PHI than the level for which they have been approved, including review of their background and clearance from Human Resources.

Workforce Member Termination of Access Policy

L. Coverage

Nightingale (hereafter referred to as the 'Organization') workforce members that access, use, disclose confidential patient information. Our workforce includes all clinical providers, clinical supportive staff involved in the care of patients, volunteers, students and other staff members involved in the routine operations of our delivery of care.

M. Review / Revision Dates

September 2014

N. Purpose

The purpose of this policy is to provide guidance on the requirements removing access to PHI for terminated employees.

O. Policy Statement

Upon termination of any the Organization's workforce members employment or upon determination of appropriate mitigation or sanctions against a workforce member their access to PHI will be eliminated or restricted immediately upon the occurrence of the triggering event. In no case shall the termination of access to PHI be delayed more than 30 minutes from the moment of such a triggering event. The Organization will document all access termination activities, in accordance with our Documentation for Privacy and Security Compliance Policy. All of these activities will be maintained a minimum of six years.

Terminating access to PHI may be tailored for voluntary, delayed terminations vs. involuntary instant terminations. In the case of voluntary terminations, ensure that removal occurs at the end of the last day of work.

NIGHTINGALE PREVENTATIVE CARE

Physical Security Policy

P. Coverage

Nightingale (hereafter referred to as the 'Organization') workforce members that access, use, disclose confidential patient information. Our workforce includes all clinical providers, clinical supportive staff involved in the care of patients, volunteers, students and other staff members involved in the routine operations of our delivery of care.

Q. Review / Revision Dates

September 2014

R. Purpose

The purpose of this policy is to provide guidance related to physical security measures that undertaken by the organization.

S. Policy

Strong physical security is mandatory part of our Organizations comprehensive security strategy. These physical security measures work with technical and administrative safeguards to protect individual identifiable patient information, including Protected Health Information (PHI). The Security Officer has overall responsibility for physical security compliance and documentation under the HIPAA Security and any other applicable regulations.

Maintenance will be performed as needed, for all physical security components listed below, including hardware, walls, doors and locks.

Areas we addressed and monitored regularly in relation to physical security include:

a. Hardware, walls, doors and locks
b. Windows and doors locks and keys and / or electronic access controls.
c. Physical security ingress and egress access points
d. Alarms, video cameras,
e. Workforce member, vendor and guest access to computing devices that contain PHI
f. Paper records (medical, billing, any others that contain PHI or sensitive information) physical security
g. Routine and non-routine deliveries
h. Physical devices for prevention of theft, logs on equipment, drawers, cabinets, files
i. Telecom, server, network desktop and mobile device physical room security

Malware Protection

T. Coverage

Nightingale (hereafter referred to as the 'Organization') workforce members that access, use, disclose confidential patient information. Our workforce includes all clinical providers, clinical supportive staff involved in the care of patients, volunteers, students and other staff members involved in the routine operations of our delivery of care.

U. Review / Revision Dates

September 2014

V. Purpose

The purpose of this policy is to provide guidance on protecting networks, software and hardware from internal and external malware programs, i.e. viruses, trojan horses and innumerable, ever changing other types of programs that can do harm to wrongful disclose all types of health information, including PHI.

W. Policy Statement

The Organization's policy is to maintain a rigorous program of processes and technologies, to prevent, detect and mitigate malicious software. It is the policy of this Organization that all of our software and networks, whether they contain PHI or not shall be protected from malware.

Malware detection shall be continuously updated and new technologies evaluated as needed.

All malware prevention software must be kept up to date with the latest definitions and similar to maintain peak protection.

Vulnerability scans and penetration testing are required by HIPAA Security rules and must be documented.

NIGHTINGALE PREVENTATIVE CARE

Login Monitoring

X. Coverage

Nightingale (hereafter referred to as the 'Organization') workforce members that access, use, disclose confidential patient information. Our workforce includes all clinical providers, clinical supportive staff involved in the care of patients, volunteers, students and other staff members involved in the routine operations of our delivery of care.

Y. Review / Revision Dates

September 2014

Z. Purpose

The purpose of this policy is to provide guidance on monitoring networks and software applications for logins and logon attempts.

AA. Policy Statement

Login monitoring is an important part of both privacy and security. It is an element of the wider scoped Access and Privacy monitoring. This Organization maintains a program of monitoring and review of log-ins and log-in attempts and related security incident reports. Possible violations or breaches of PHI, along with other potentially inappropriate or illegal activities shall immediately be brought to the attention of the compliance chain of command as well as possibly legal counsel, and/or Human Resources. All procedures, timing, monitor findings, investigations of events (incidents) shall be documented and retained for the regulatory timeframe.

NIGHTINGALE PREVENTATIVE CARE

Password and Logon Management

BB. Coverage

Nightingale (hereafter referred to as the 'Organization') workforce members that access, use, disclose confidential patient information. Our workforce includes all clinical providers, clinical supportive staff involved in the care of patients, volunteers, students and other staff members involved in the routine operations of our delivery of care.

CC. Review / Revision Dates

September 2014

DD. Purpose

The purpose of this policy is to provide guidance on issuing and maintaining passwords and logon credentials for the organization's computer systems.

EE. Policy

Workforce members who access PHI or any confidential organizational information must utilize secure passwords and logon credentials..

All passwords, logon credentials and associated items such as reminders and systems for password retrieval are to be secured via the use of 'strong' passwords. Passwords and logons should be changed for each user at least annually.

Do not leave passwords or logon credentials in plain sight and refrain from storing them in easily accessible, public or locations where they could be stolen.

HIPAA training and security awareness programs will include password management as a topic.

Password Tips

6 or 8 digit letter-number combination

Strong passwords are preferred

- Passwords changed every 6 months
- Password enabled systems set for automatic reminders every 6 months
- Do not use obvious passwords personal of family information
- Do not write down or store the passwords in office or near your computer
- Do not use 'remember password' features

Management of Reported Security or Privacy Events (Incidents)

FF. Coverage

Nightingale (hereafter referred to as the 'Organization') workforce members that access, use, disclose confidential patient information. Our workforce includes all clinical providers, clinical supportive staff involved in the care of patients, volunteers, students and other staff members involved in the routine operations of our delivery of care.

GG. Review / Revision Dates

September 2014

HH. Purpose

The purpose of this policy is to provide guidance on reporting, investigating and documenting security or privacy events (which also may be referred to as 'incidents' or 'suspected violations').

II. Policy Statement

This organization will appropriately respond in a timely manner to all security and privacy events, regardless of their severity. The responsibility for management of security or privacy events (incidents) response resides with the Privacy and Security Officers. Specific procedures and forms have been created for response to any significant events. Regardless of the mechanism by which the event is reported, this documentation will be kept for a minimum of the HIPAA 6 year timeframe.

- New hire and on-going security and privacy training and awareness programs for workforce members must include security (and privacy) event (or incident) reporting.

NIGHTINGALE PREVENTATIVE CARE

Emergency Access

JJ. Coverage

Nightingale (hereafter referred to as the 'Organization') workforce members that access, use, disclose confidential patient information. Our workforce includes all clinical providers, clinical supportive staff involved in the care of patients, volunteers, students and other staff members involved in the routine operations of our delivery of care.

KK. Review / Revision Dates

September 2014

LL. Purpose

The purpose of this policy is to provide guidance on gaining emergency access to critical EHR (electronic health record) systems and other computer systems, all of which contain crucial patient and / or operational data needed in many ways, but especially for patient care, especially in an emergent situation.

MM. Policy Statement

Emergency access procedures for clinical EHR and other key Organizational computer systems have been created while maintaining full compliance with HIPAA regulations. These emergency access procedures may include access to PHI (Protected Health Information These procedures have been developed to ensure that authorized workforce members can access appropriate health information, including during emergencies.

These emergency accesses are intended to provide providers of care and other supporting staff with access to PHI and related health information especially to allow uninterrupted health care delivery, even in times when normal security procedures cannot be followed. There may also be emergency access to the Organizations computer systems by any party needed to make crucial, real time decisions and actions to maintain the computers, the data they manage and to document healthcare. All emergency access will be logged with the user information and reasons for the emergency access. These accesses will be reviewed by appropriate compliance governance on a routine basis.

NIGHTINGALE PREVENTATIVE CARE

Business Continuity

NN. Coverage

Nightingale (hereafter referred to as the 'Organization') workforce members that access, use, disclose confidential patient information. Our workforce includes all clinical providers, clinical supportive staff involved in the care of patients, volunteers, students and other staff members involved in the routine operations of our delivery of care.

OO. Review / Revision Dates

September 2014

PP. Purpose

The purpose of this policy is to provide guidance on the organizations data criticality, back-up, emergency operational preparedness and business continuity measures.

QQ. Policy Statement

Business Continuity

An overarching business continuity strategy is required to ensure timely access to health information by providers of care on a continuous, every day basis. There are multitudes of threats to the integrity and accessibility of the Organization's health information. Power issues or outages, fire, flood, other natural or manmade disaster, viruses, hackers, and improper acts by employees and others all introduce risk into the management of key clinical, financial and operational health information. Responsibility for planning and executing contingency operations shall reside with Privacy and Security Officer.
The following conditions can destroy or disrupt the Organization's information systems:

- Power interruption or outage
- Fire
- Water
- Weather and other natural phenomena, such as earthquakes
- Sabotage and vandalism
- Terrorism

NIGHTINGALE PREVENTATIVE CARE

Hardware & Media and Mobile Device Management

RR. Coverage

Nightingale (hereafter referred to as the 'Organization') workforce members that access, use, disclose confidential patient information contained on computers and digital devices. Our workforce includes all clinical providers, clinical supportive staff involved in the care of patients, volunteers, students and other staff members involved in the routine operations of our delivery of care.

SS. Review / Revision Dates

September 2014

TT. Purpose

The purpose of this policy is to provide guidance on the management of this Organization's hardware, digital media and mobile devices to prevent wrongful access, use or disclosure of electronic PHI (ePHI) or otherwise sensitive information or data these devices may contain. This policy also addresses the use of personal devices to manage PHI or sensitive organizational data.

UU. Policy

Management of the computer hardware, digital media and digital mobile devices including but not limited to such as iPhones, Smart Phones, iPads, Flash drives present unique challenges and risks to the security and privacy of any sensitive information or PHI (ePHI) accessed, used, stored within them. These risks can be minimized by establishing appropriate controls and implementing the necessary measures for optimal protections. This Organization's policies and procedures are to be clearly communicated and enforced for all workforce members to establish expectations and convey accountability.

Hardware and more portable and re-useable digital recording and storage media containing individually identifiable health information, including PHI (Protected Health Information) or other sensitive information must be properly erased, encrypted, or completely destroyed to prevent any data the device contains to be unusable and irrecoverable in the event of theft, loss, misuse. Re-use of media is not allowed unless appropriate erasure and updating is applied

Encryption and decryption of data in all kinds of digital devices, including, but not limited to those that are portable or re-useable shall be undertaken in compliance with the organization's strategic IT plan. Data encryption should be managed according to HIPAA Security and NIST compliance regulations to prevent wrongful access, use and disclosure of PHI and other types of sensitive information.

All hardware, media and mobile devices will have all data erased in compliance with HIPAA regulations prior to transfer of ownership (sale, donation or trade) or disposal of the devices, including, but not limited to copiers, medical devices, computers, phones, flash drives, etc. Media will be erased before re-use by another user.

Automatic Log-off

A. Coverage

Nightingale (hereafter referred to as the 'Organization') workforce members that access, use, disclose confidential patient information. Our workforce includes all clinical providers, clinical supportive staff involved in the care of patients, volunteers, students and other staff members involved in the routine operations of our delivery of care.

B. Review / Revision Dates

September 2014

C. Purpose

The purpose of this policy is to provide guidance on the use of automatic log-off features within this Organization's IT systems.

D. Policy Statement

Usage of automatic log-off for any computer system containing PHI or other sensitive information is a crucial part of this Organization's security program. All computer systems in use within this organization must utilize automatic log-off procedures.

Settings and timings shall be as uniform as possible within the organization, across the various IT systems. Workstation log-off, especially in patient / public facing areas, should occur within a very few minutes, according to defined procedure.

Responsibility for the development and implementation of automatic log-off policies and procedures associated reside with the Privacy and Security Officer. All automatic log-off procedures shall be documented in accordance with the Documentation for Security and Privacy Compliance policy.

Workstation Security and Use

VV. Coverage

Nightingale (hereafter referred to as the 'Organization') workforce members that access, use, disclose confidential patient information. Our workforce includes all clinical providers, clinical supportive staff involved in the care of patients, volunteers, students and other staff members involved in the routine operations of our delivery of care.

WW. Review / Revision Dates

September 2014

XX. Purpose

The purpose of this policy is to provide guidance on the security and use of the computer workstations within this Organization.

YY. Policy Statement

This Organization's policy and procedure development combined with workforce training about the security and use of computer workstations is a crucial element in our IT security program. Workstation security procedures and their proper use help maintain the confidentiality for all PHI (Protected Health Information) and sensitive information within this organization.

Workstation Security includes physical security such as not placing computers in patient areas unless they are secured behind desks into more easily monitored and simple security by our workforce to constantly be vigilant, watching over our resources, including computer workstations.

Specific procedures shall be developed to implement physical safeguards for all workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), to restrict access to authorized users only.

NIGHTINGALE PREVENTATIVE CARE

User Authentication and Unique User ID

ZZ. Coverage

Nightingale (hereafter referred to as the 'Organization') workforce members that access, use, disclose confidential patient information. Our workforce includes all clinical providers, clinical supportive staff involved in the care of patients, volunteers, students and other staff members involved in the routine operations of our delivery of care.

AAA. Review / Revision Dates

September 2014

BBB. Purpose

The purpose of this policy is to provide guidance on user authentication to ensure only persons entitled to access, use or disclosure Organizational PHI and sensitive information are allowed to logon to the computers and digital devices that contain them.

CCC. Policy Statement

Unique user I.D.'s for logons to all computers and digital devices is required by this organization in compliance with HIPAA Security rules and to maintain PHI and sensitive information's privacy. These unique ID's serve to authenticate users identities and to deny imposters access. Each user must always be individually identified (authenticated) by their logon credentials in order to accurately account for and track acceptable and wrongful access, use and disclosure of PHI or sensitive information.

Conditions of use of passwords / logon credentials are addressed within the Confidentiality and Security Agreement. All workforce members, Business Associates, Contractors or other parties that have lawful access to information with this Organization's computers and digital devices must sign a Confidentiality and Security Agreement prior to being issued passwords and logon credentials. Sanctions will be applied, for violations to this Agreement.