FOR MUNSON USE ONLY

If used as template, MUST change name of agency and details to reflect YOUR practice

Name of Policy: Breach Incident Management and Breach Notification Policy

PURPOSE:

The purpose of this policy is to guide Munson's response to any privacy or security breach complaint, report or audit in accordance with the regulations and recommendations as defined in Privacy and Security Standards of the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, 45 CFR Parts 160 and 164, as they are amended from time to time (collectively "HIPAA").

The HIPAA Omnibus Rule**,** effective March 26, 2013 significantly expanded the privacy and security requirements under HIPAA. HIPAA defines a breach as the acquisition, access, use or disclosure of protected health information in a manner not permitted under the HIPAA Privacy Rule, which compromises the security or privacy of the Protected Health Information (PHI). The Final Rule replaces the "harm threshold" used in the Interim HIPAA Rule with a presumption that that any acquisition, access, use or disclosure of PHI not permitted under the Privacy Rule would be considered a breach unless the covered entity or business associate could demonstrate that there is a low probability that, based on a risk assessment, the PHI had been compromised.

POLICY:

It is Munson's policy to protect the privacy and security of PHI in compliance with applicable Federal and State law, as well as with Munson policies and procedures. It is Munson's policy to foster a culture of respect for patient privacy and to prevent (PHI) from being compromised. Munson's Privacy Officer and/or Security Officer will thoroughly investigate, document, report and work with department managers and Human Resources to mitigate all incidents, including suspected or known violations of privacy and security, in a timely manner.

This policy clarifies privacy and security breach incidence response process, supports Munson's sanctions policy, Confidentiality and Systems Usage Breach, #001.048 and incorporates Munson's procedural guides on Breach Notification and Large Scale Incidence Response.

BREACH EXCEPTIONS

Exception to the HIPAA definition of breach includes:

1) Any unintentional acquisition, access, or use of PHI, by a workforce member or authorized person, made in good faith and within the scope of authority and if there is no further impermissible use or disclosure,

2) Any inadvertent disclosure of PHI by a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same organization (or organized health care arrangement in which the covered entity participates) and the PHI is not further impermissibly used or disclosed and,

3) A disclosure of PHI where the covered entity or business associate has a good faith belief that the unauthorized recipient would not reasonably have been able to retain the information.

4) An incident where the PHI was secured, i.e. encrypted (in motion or at rest) or rendered unreadable, i.e. shredded.

Note:

a. Date of birth and zip code are no longer included in the exceptions list for limited data set and are now considered PHI.
b. Violation of HIPAA's minimum necessary standard is now a reportable breach. Covered entities and business associates must make *reasonable efforts* to limit PHI to the minimum necessary. However, of a request for PHI is received from another business associate, or covered entity, since the request itself must be limited to the minimum necessary, Munson may reasonably rely on the request as requesting the minimum necessary for the disclosure.
c. The exceptions to the minimum necessary standard have not changed:

Disclosures to or requests by a provider for treatment;
Uses or disclosures made to an individual;
Uses or disclosures made pursuant to an authorization;
Disclosures made to the Secretary of the Department of Health and Human Services (HHS);
Uses or disclosures that are required by law; and
Uses and disclosures required for compliance with the privacy rule.

IMPLEMENTING PROCEDURE

Organizational Structure for Incident Management

1) For breaches affecting less that twenty-five individuals, the Privacy Officer may seek risk assessment consultation from a risk assessment team comprised of the audit team, Security Officer, Risk Management and/or Legal Counsel; in simple cases, the Privacy Officer may investigate and draw conclusions independently.

2) For breaches affecting more than twenty-five individuals, including large scale breaches affecting over 500 individuals, the Privacy Office will convene the large scale Incident Response Team comprised of Information

Systems, Human Resources, Corporate Compliance, Corporate Communications, Security, and Legal Counsel.

Representatives from the risk assessment team and/or the Privacy Officer will determine probability of risk of harm to PHI. Minimally, the following factors will be asked and answered:

1) Whether the acquisition, access use or disclosure of the PHI violates the HIPAA Privacy Rule,
2) Whether the PHI involved was "unsecured," (usable, unreadable or indecipherable/encrypted)
3) Whether an exception to the definition of breach may apply, and
4) Whether there was a low probability that the PHI has been compromised.

A risk assessment to determine whether there is a low probability that the PHI has been compromised must include consideration of the following four factors:

1) The nature and extent of the PHI involved, including the types of identifies and the likelihood of re-identification.
2) The unauthorized person who used the PHI or to whom the disclosure was mad,
3) Whether the PHI was actually acquired or viewed, and
4) The extent to which the risk to the PHI has been mitigated.

The risk assessment team and/or Privacy Officer will work toward **remediation and prevention of reoccurrence on breach.** Numerous steps may be used to remediate the effects of the breach, such as:

1) Offering credit monitoring to the affected individuals in the event that Social Security number or financial account data are involved in the breach,
2) Setting up a call center to address questions of affected individuals regarding the breach,
3) Improving existing policies or procedures,
4) Additional training of workforce members on how safeguard PHI,
5) Encrypting portable media that contains PHI,
6) Requiring employees to change their passwords,
7) Increasing physical security through the use of biometric locks or other devices
8) Sanctions to employee who violated breach policy, ranging from re-education to written warning, to termination.

9) And in particular, identifying any gaps in compliance that led to the breach and closing those gaps to ensure that another similar breach will not occur.

The Privacy Officer notifies employee's manager after learning about a breach, for their help in coordinating efforts in the investigation. All breaches attributable to Munson employees are reported to Human Resources and the employee's manager. If a physician is suspected of a breach, the Privacy Officer coordinates the investigation with the Medical Director of Information Systems. Munson's Privacy Office receives reports of, investigates, audits, documents and reports on suspected or actual violations of privacy and security policies and procedures. The Privacy Office documents and retains information about both privacy and security incidents and their investigation results, including the risk assessment process and results, breach notification letters, and follow up regarding sanction to employee.

For reportable breaches, the Privacy Officer writes breach notification letters as soon as possible, but no later than within 60 days of learning of breach, and annually notifies Health and Human Services (HHS) for those breaches affecting less than 500 individuals. For large scale breaches, Privacy Office notifies HHS within 60 days of learning of breach. Corporate Communications will determine media notification; call center set up and web presence to answer public concerns regarding a large scale breach within 60 days, in compliance with HIPAA guidelines (see below). The Incident Response Team debriefs each larger breach occurrence to initiate further analysis, determine root cause, and perform a "gap analysis" of where policy or procedure needs to be strengthened and other measures as needed to prevent reoccurrence.

The Privacy Office and Security Office periodically produce periodic reports and perform trend analyses of incidents for administrative review, including the Security Review Board.

Human Resources, Departmental Managers and Privacy (and Security Officer as appropriate) will assess all violations and review disciplinary action options, based on the Sanctions Policy, to make recommendation of appropriate disciplinary action for employees. Physician Leadership groups will determine appropriate disciplinary consequences per established Medical Executive Board rules, with input from the Medical Director of Information Systems and the Privacy Office.

Reporting Incidents

It is the responsibility of Munson workforce members, business associates, or any other external person who has been authorized to have access to Munson's network, systems, applications or data, to report any known or suspected privacy or security incident involving PHI to Munson's Privacy Office or Security Office.

Suspected or actual incidents may be identified and reported from a number of different sources including, but not limited to, patients, their families or friends; workforce members; physicians; business associates; occurrence or auditing reports; IS staff; regulatory agencies.

These incidents may be reported directly to the Privacy Officer but often they are initially reported to clinicians, supervisors, the Help Desk, application teams, VOICE reporting system, Risk Management, Legal, executive management, or patient liaisons. **The date for breach notification begins when someone in agency is aware of event, or should have been aware, using reasonable diligence. It is the responsibility of those individuals and departments who receive reports of incidents to forward them to the Privacy Office in a timely manner.**

Mandatory Notification Requirements – Reporting to HHS

- Immediate notification of HHS must be made concerning Breaches of Unsecured PHI impacting more than 500 individuals.
- For Breaches of Unsecured PHI impacting fewer than 500 individuals, the Privacy Officer will document the breaches in Feedback Monitor Pro or other complaint management form.
- Using the data entered into Feedback Monitor Pro, or other incident documentation systems the Privacy Office will submit the required notification to HHS no later than sixty (60) days after the end of each calendar year. One form per each incidence is submitted.

Mandatory Notification Requirements – Reporting to Media

- Corporate Communications: the content of the media notification shall include:

    - A brief description of the occurrence, including the date of the Breach and the date of discovery;
    - A description of the types of unsecured protected health information involved (e.g., SSN, full name, DOB, etc.);
    - Steps individuals should take to protect themselves from further harm;
    - A brief description of Munson's efforts to investigate the Breach, mitigate losses and protect against further Breaches; and
    - Contact procedures for questions which shall include a toll-free number, an e-mail address, website OR postal address.

Initial Incident Response

When an incident is discovered, any necessary immediate corrective action will be initiated to prevent the incident from continuing and to minimize and contain potential damage.

The Privacy Officer will document initial information about the incident.

Incident information documentation will include: Type of incident; description of the incident; type and extent of PHI involved, number of persons affected, identification of the network and major applications, systems and/or databases impacted; date of occurrence; date reported; the name of the person who reported the incident and the person to contact for more information; names of persons affected, names of persons/positions that have been notified of the incident. Other relevant information will be added, including all follow up investigative and remedial actions taken.

Incident Investigation

The Privacy Officer gathers evidence about the incident and documents the progress of the investigation.

If the breach is a security incident, collecting evidence may involve: making backup copies of damaged or altered files and keeping them in a secure, off-line location; reviewing audit trails; continuous monitoring of system activity, disconnecting the affected system from the network and/or shutting down the system; restricting all users' access to a compromised system; deletion of a specific user's access privileges; and reviewing system security configurations.

If it is a privacy incident, this may involve interviewing patients, workforce members or others; obtaining monitoring reports of accesses to the PHI in question; chart review by Privacy Officer, conducting specific auditing reports, reviewing access privileges; obtaining Help Desk records of reported problems; checking work documents used; checking employee files for evidence of training; or other steps.

If the incident involves a business associate of Munson, the Privacy Officer will notify the office manager who is responsible for the business relationship with the vendor and may serve as a consultant to him/her throughout the investigative process. The Business Associate will send a copy of the Breach Notification letter to Munson's Privacy Office for approval, as clarified in the Business Associate Agreement.

1. For breaches affecting less than 25 individuals the risk assessment team will evaluate the extent of harm or potential harm done to:

the patient; the integrity of the PHI, the systems, applications, databases, and network; to Munson's reputation, financial position or market advantage.

2. For breaches affecting greater than 25 individuals and 500+ individuals the incident response team will review investigative data, seek to contain the damage, gather additional facts, determine notification requirements, prepare a response strategy, develop a corrective action plan, implement the plan, and monitor the corrective action plan.

Patient/Complainant Mitigation

Munson will take positive and reasonable actions to correct or minimize any identified privacy or security violation impacting a patient, weighing the possible negative impact a breach notification letter may have on the patient, and whether the probability of risk to PHI is so low as to outweigh the benefits of notifying patient and having an unnecessary and stressful reaction to letter.

a. Upon successful resolution of the complaint, the Privacy Officer will provide the patient with a letter documenting the resolution, in accordance with Complaint Management policy for policy breaches. Privacy breach notification letters will follow the template guideline as provided by Health and Human Services. The notification should be made via First Class Mail. Another appropriate method may be utilized where cases include insufficient or out-of-date contact information exists in accordance with HIPAA. A courtesy phone call prior to mailing notification letter may occur. The notification shall include:

    - A brief description of the occurrence, including the date of the breach and the date of discovery;
    - A description of the types of unsecured protected health information involved (e.g., SSN, full name, DOB, etc.);
    - Steps individuals should take to protect themselves from further harm;
    - A brief description of the organization's efforts to investigate the breach, mitigate losses (i.e., credit monitoring) and protect against further breaches; and
    - Contact procedures for questions which shall include a toll-free number, an e-mail address, website OR postal address.

Organizational Remediation

The Privacy and Security Officer and other management personnel, along with the Incident Response Team and Security Review Board, will evaluate each incident in terms of the strength of the controls in place to prevent re-occurrence of this type of incident.

The Privacy Officer and or Human Resources will determine HIPAA education needs for the employee involved in beach and inform the

manager in the appropriate department. Security improvements will be under the authorization of the IS Director and Security Officer. If controls are weak or if workforce members are not properly trained, the Privacy Official will inform the manager in the appropriate department and make recommendations for re-education.

Disciplinary Action

For incidents involving misconduct by Munson workforce members, the Privacy Office will discuss the results of the investigation with the Human Resources Director and the workforce member's manager and will recommend an appropriate disciplinary action consistent with Munson sanctions policy and other Human Resource policy. This is a recommendation only, as final authority rests with Human Resources.

For incidents involving members of Munson's medical staff, the Privacy Officer will notify the MDIS and assist in obtaining investigative reports and audits. The Medical Leadership Committee will make disciplinary recommendation to the Medical Executive Committee for determination of appropriate disciplinary action according to their bylaws.

For incidents involving independent office staff, the physician office manager will determine the necessary disciplinary actions, including re-education, to written warning to termination. Appropriate sanctions are addressed in the BAA.

Notification/Ongoing Communication

Patients and others who make a complaint about a privacy or security incident will be informed about Munson's incident investigation process and notified in a timely fashion about the receipt of their complaint and the status of the investigation.

The Privacy Office will oversee auditing and notification plan for informing appropriate internal management and staff about known or suspected incidents.

Correspondence with outside authorities such as OCR, local police and the FBI regarding privacy or security incidents will be handled by the Privacy Office, after consultation from Legal and/or Risk Management departments.

Privacy and Security incidents will be reported to Administration periodically; incidents affecting over twenty five individuals will be reported immediately to Administration and to Information Systems Director.

Privacy Office will report letters received from Office of Civil Rights regarding privacy complaints to Information Systems Director and Legal

Counsel and will coordinate a response to Office of Civil Rights in collaboration with Legal Counsel.

Document Retention

All documents (information collected on each privacy and security incident, etc.) required under this procedure will be retained, at a minimum, for six (6) years from the date of their creation or the date when they were last effective, whichever is the latest date. No documents will be destroyed before consultation with Privacy Office and/or legal counsel.