1. PURPOSE AND SCOPE

1.1 This policy and procedure sets forth the Fire Department’s breach notification requirements in the event of an unauthorized acquisition, access, use, or disclosure of unsecured patient health information, including unsecured patient health information protected pursuant to the federal Health Insurance Portability and Accountability Act (HIPAA) and the Privacy Regulations promulgated thereunder (“HIPAA Regulations”), and the federal Health Information Technology for Economic and Clinical Health Act (HITECH) and the regulations promulgated thereunder (“HITECH Regulations”).

1.1.1 This policy and procedure applies to all:

- Fire Department Emergency Medical Service personnel;
- Fire Department uniformed firefighting personnel who provide
- Certified First Responder-Defibrillation (CFR-D) patient care;
- All other Fire Department personnel who have access to, use, maintain or disclose patient health information or employee health records, including those assigned to perform investigative, legal, medical, operational, revenue, privacy and recordkeeping management, oversight and other functions.
- Any Fire Department personnel who become aware of any unauthorized use or disclosure of Fire Department patient health information or any breach of this policy.

1.2 This policy and procedure applies to all Fire Department information and records the confidentiality, use and disclosure of which is governed by the Fire Department’s “Confidentiality, Use and Disclosure of Patient Health Information” policy, A.U.C. 334/EMSC OGP 113-05. (The HIPAA Regulations and HITECH Regulations make use of the term “protected health information” to refer to the patient information of “covered entities” subject to the regulations. To avoid any confusion as to whether and which patient information is “protected,” this policy and procedure instead uses the term “patient health information,” to refer to any and all information relating to the patient or patient treatment or transport.)

2. HITECH BREACH NOTIFICATION REQUIREMENTS

2.1 The HITECH Act, part of the American Recovery and Reinvestment Act of 2009 (ARRA), and the HITECH Regulations establish notification requirements to report the breach of confidentiality by loss or theft of patient information that is not protected by encryption.
2.2 The breach notification obligations of HITECH require that health care providers and other “covered entities” under HIPAA notify patients of any breach of the privacy of their identifiable protected health information. Covered entities are also required to notify the United States Department of Health and Human Services (“DHHS”) and in some instances, the broadcast media.

2.3 “Unsecured” protected health information is defined as patient health information that is not protected through a technology or methodology that makes the protected health information unusable, unreadable or in some way indecipherable to persons not authorized to have the information (consistent with HITECH Regulations). Unsecured information may be in electronic or hard copy form, or in the form of verbal communication (speaking).

2.4 A “breach” is generally defined as the acquisition, access, use or disclosure of unsecured protected health information in a manner not otherwise permitted by the HIPAA Regulations that compromises the security or privacy of the protected health information by posing a significant risk of financial, reputational or other harm to the affected individual.

2.5 A breach may occur through accidental or affirmative means. For example, a breach may occur:

- accidentally, such as when a laptop or storage device containing patient health information is lost or stolen; or
- affirmatively but unknowingly, such as when an employee accesses, uses or discloses patient health information when not authorized to do so, because the employee did not know the information was confidential and must be kept confidential; or
- affirmatively and knowingly, such as when an employee intentionally makes unauthorized use of patient health information for personal or other reasons.

Accordingly, the covered entity must put in place the appropriate safeguards limiting access, and employees must exercise care in their handling of patient health information.

2.6 HIPAA Regulations require that covered entities enter into a Business Associate Agreement with each contractor that receives and stores the covered entity’s protected health information. The HITECH Regulations require the business associate to secure such protected health information and protect it from disclosure to the same degree as the covered entity and requires the Business Associate to report a breach of the confidentiality of protected health information to the covered entity.

3. POLICY

3.1 It is the policy of the Fire Department to preserve the confidentiality of patient health information and to use and disclose such information only for such purposes as are authorized by law and regulation.

3.2 All Fire Department personnel who obtain, maintain, use and/or have access to patient health information, including patient communications and patient care documentation, are required to preserve the confidentiality of such information and shall only use and disclose such information in accordance with the Fire Department’s Confidentiality, Use and Disclosure of Patient Health Information policy.
3.3 It is the policy of the Fire Department to immediately address any situation that gives rise to a breach of the confidentiality of patient health information.

3.4 It is the policy of the Fire Department to report any such breach in a manner fully consistent with the law.

3.5 In the event of a breach, it is the policy of the Fire Department to prevent any recurrence or other future breach of confidentiality by reviewing its confidentiality and security policies and procedures to identify and address any deficiencies.

3.6 Adherence by Fire Department personnel with the provisions of this policy and procedure will ensure compliance with the breach reporting requirements of the HITECH Regulations.

4. IDENTIFICATION AND REPORTING TO FIRE DEPARTMENT CONFIDENTIAL COMPLAINT UNIT OF A BREACH OF CONFIDENTIALITY OF PATIENT HEALTH INFORMATION (ALL FIRE DEPARTMENT PERSONNEL AND CONTRACTORS)

4.1 Any Fire Department personnel or contractor who discovers a breach of confidentiality of Fire Department patient health information shall immediately report such breach by notifying the Fire Department’s Confidential Complaint Unit (CCU), which has been designated to receive such notifications. “Immediate” reporting of a breach means as soon as can be safely undertaken without disrupting agency operations, but in no event later than the end of the workday or tour of duty.

4.2 A report of a breach of confidentiality shall be made by e-mail, if e-mail access is available, or, if e-mail access is unavailable, by telephone communication to the CCU at (718) 999-2646, followed by submission of a written report within 24 hours of such telephone notification.

4.3 A report of a breach of confidentiality shall include the nature and circumstances of the breach, and identify the patient health information or records that were accessed or disclosed (for example, a Patient Care Report, a Medical Folder or a disk or drive containing identifiable patient health information). The report shall indicate the patient’s identity, if known. If the breach affects many patients, the report shall include an estimate of the number of affected patients.

4.4 Fire Department personnel reporting a breach of confidentiality should copy their bureau head or the commanding officer of their station or unit on the immediate report and any follow-up report. To minimize any further dissemination of the disclosed patient health information, no other persons shall be copied on the report except as may be necessary to ensure prompt attention to the report (such as if the bureau head or commanding officer is or will be absent from the office).

4.5 If the breach involves lost or stolen equipment, such as a laptop computer, flash drive or Blackberry, such loss or theft should be reported in accordance with regular Fire Department procedures.
5. NOTIFICATION OF PATIENT OF BREACH OF CONFIDENTIALITY (PRIVACY BREACH RESPONSE TEAM)

5.1 Reported breaches of the confidentiality of patient health information shall be investigated, and any necessary or appropriate remedy implemented, by the CCU, the Privacy Officer, the Bureau of Legal Affairs and/or other appropriate Fire Department personnel, separately or collaboratively, as circumstances warrant (“Privacy Breach Response Team”).

5.2 Upon receipt of a report of a breach of confidentiality, the Privacy Breach Response Team shall promptly investigate the nature and circumstances of the breach, the patient health information or records were accessed or disclosed, and the identity of the affected patient(s).

5.3 To determine if a reportable breach has occurred, the Privacy Breach Response Team shall conduct a risk assessment to determine if, and to what extent, if any:

- the security or privacy of patient health information has been compromised (including whether or not the information was deidentified or encrypted);
- whether the patient health information was information protected by HIPAA and HITECH;
- there is a significant risk of financial, reputational or other harm to the affected patients as a result of unauthorized access to, or use or disclosure of, unsecured protected health information;
- the person who gained unauthorized access to the patient health information would reasonably be able to retain such information; and
- the unauthorized access or disclosure is subject to certain exceptions to breach notification requirements.

5.4 If the Privacy Breach Response Team determines that identifiable patient health information was accessed, used or disclosed, and there is a significant risk of harm to the affected patient(s), then a breach notification must be made to the patient in accordance with the HITECH Regulations.

5.5 Notification of a reportable breach of confidentiality shall be made to each affected patient (or their personal representative or next of kin, as appropriate) without “unreasonable delay,” but in no case later than 60 days of discovering the breach. In accordance with the HITECH Regulations, a breach is considered “discovered” as of the first day on which the breach is known by any employee or agent of the covered entity or should have been known to the covered entity if it had exercised “reasonable diligence.”

5.6 Notification of a reportable breach of confidentiality shall be provided by regular first class mail to the last known address of the patient, unless the person has indicated a preference for e-mail communications. If it appears that there will be imminent misuse of unsecured patient health information, notification may be provided by faster means, if feasible, such as telephone or email in addition to the written notice.
5.7 Notification of the breach shall be communicated in plain, easily understandable language, and include the following information:

- A brief description of what happened (e.g., laptop containing unencrypted patient health information stolen from office), including the date of the breach and the date of the discovery of the breach (to the extent that the information is known);

- A description of the type of unsecured patient health information that was disclosed (e.g., Patient Care Report);

- Steps that the recipient should take to protect themselves from potential harm result from the breach (such as contacting credit card companies to alert them to monitor the account for fraudulent activity);

- A brief description of the actions taken to investigate the breach, mitigate any harm resulting from the breach, and to protect against further breaches; and

- Contact information (such as a website address or telephone number of an appropriate representative) from which or whom the recipients can obtain additional information.

5.8 If the address of one or more of the affected patients is not known, notification of a breach of confidentiality shall be made in the following manner:

- If the addresses of fewer than 10 affected patients are unknown, the Privacy Breach Response Team shall provide substitute notice by other means reasonably calculated to reach the affected patients, such as by telephone.

- If the addresses of 10 or more affected patients are unknown, the Privacy Breach Response Team shall provide substitute notice by a conspicuous posting on the Fire Department’s website for 90 days or by publication of a conspicuous notice in a local major print or broadcast media outlet (unless there is reason to believe the affected individuals do not reside in New York City). The substitute notice shall include a toll-free telephone number which recipients can call for at least 90 days to obtain additional information.

6. NOTIFICATION OF BROADCAST MEDIA OF BREACHES OF CONFIDENTIALITY (PRIVACY BREACH RESPONSE TEAM)

6.1 If the breach affects more than 500 patients, the Privacy Breach Response Team shall also provide notice to major media outlets in the New York City area. The notice shall contain the same information as the written notice to the affected individuals and be given without unreasonable delay, but not later than 60 days after discovery of the breach.

7. BREACH RECORDKEEPING (PRIVACY BREACH RESPONSE TEAM)

7.1 The Privacy Breach Response Team shall maintain a record of all breaches of confidentiality reported to CCU; the total number of affected patients, clearly distinguishing between breaches involving those affecting less than 500 individuals and those affecting 500 or more individuals; the Privacy Breach Response Team’s determination as to whether notification of the breach to affected patients is required; and if required, the date(s) and method(s) by which such notification was made.
8. NOTIFICATION OF DHHS OF BREACHES OF CONFIDENTIALITY (PRIVACY BREACH RESPONSE TEAM)

8.1 If the breach of confidentiality affects 500 or more patients, the Privacy Breach Response Team shall notify DHHS simultaneously with the notification to the affected patients.

8.2 If fewer than 500 individuals are affected the Fire Department will submit a log of such breaches to DHHS annually, within 60 days of the end of the calendar year.

9. BREACHES OF CONFIDENTIALITY BY BUSINESS ASSOCIATES (BUREAU OF FISCAL SERVICES AND PRIVACY BREACH RESPONSE TEAM)

9.1 The Bureau of Fiscal Services shall ensure that any organization that receives from the Fire Department protected health information subject to HIPAA and HITECH enters into a business associate agreement with the Fire Department.

9.2 A business associate agreement with a Fire Department contractor shall require the contractor to protect the Fire Department’s protected health information to the same degree as the Fire Department and to report any breach of confidentiality of the protected health information to the Fire Department.

9.3 The business associate shall report such breach of confidentiality to the CCU or other Fire Department representative designated in their Fire Department contract without unreasonable delay and in no case later than 30 calendar days after discovery of a breach. If the report is made to another Fire Department representative, such Fire Department representative shall immediately report the breach to the CCU in accordance with this policy and procedure.

9.4 Reports of breaches of confidentiality by Fire Department contractors shall be reviewed, investigated and evaluated, and notifications made, in accordance with this policy and procedure.

10. ENFORCEMENT

10.1 Any Fire Department personnel or contractor who fails to report to the CCU, in accordance with the provisions of this policy and procedure, a breach of confidentiality of patient health information may be subject to disciplinary action, up to and including termination of employment, or other appropriate enforcement action.

10.2 No Fire Department personnel or contractor shall retaliate against any employee or other personnel for reporting a breach of confidentiality of patient health information in accordance with the provisions of this policy and procedure.

10.3 Unauthorized access to, use or disclosure of, patient health information may be subject to disciplinary action, up to and including termination of employment, in accordance with the Fire Department’s Confidentiality, Use and Disclosure of Medical Information policy, or other appropriate enforcement action.

BY ORDER OF THE FIRE COMMISSIONER AND CHIEF OF DEPARTMENT