TITLE: CONSORTIUM-PSO Data Security Policies and Procedures

EFFECTIVE DATE: September 1, 2009 and revised September 1, 2010

Purpose:

To create data security policies and procedures with respect to PSWP for the operation of the Consortium-PSO in accordance with the Patient Safety Act and, as applicable, the HIPAA Privacy Rule.

Policy:

The Consortium-PSO shall develop written policies and procedures to address each of the data security considerations with respect to PSWP specified in the Patient Safety Act, including but not limited to those included in 42 C.F.R. §3.106. In addition, the Consortium-PSO shall develop written policies and procedures that address the security requirements in the HIPAA Privacy Rule, to the extent applicable.

Procedures:

(1) The Consortium-PSO shall secure PSWP in accordance with the security management requirements set forth in 42 C.F.R. §3.106, as may be amended from time to time, and the Consortium PSWP Policy.

(2) The Consortium-PSO shall adhere to these requirements at all times and at any location at which the Consortium-PSO, its workforce members, or its contractors receive, access, or handle PSWP. Handling PSWP includes its processing, development, use, maintenance, storage, removal, disclosure, transmission and destruction.

(3) The Consortium-PSO shall receive PSWP from participating healthcare providers through the IHA website. This PSWP will be housed separately on an IHA contracted server and Consortium-PSO staff will access it remotely. Passwords will be required to access this data. IHA will be contractually obligated to manage such passwords and to ensure that the data collection and storage meets the standards enunciated in the Patient Safety Act.

(4) If Consortium-PSO receives PSWP from a participating healthcare provider in a manner other than above, the Consortium-PSO or its contractors will input the data via the IHA website and previous files or paper will be destroyed.

(5) The environmental scanning project that the Consortium-PSO will initiate in 2010 will include site visits and the development of a common survey tool for participating
providers. This data will be collected and stored in conformance with the Patient Safety Act and will constitute PSWP.

(5) In general, paper PSWP, where practical and appropriate, will be scanned into electronic form and housed on IHA’s PSWP server with timely destruction of the paper PSWP.

(6) If it is necessary for the Consortium-PSO to have any paper PSWP, it will be stored in a secured file and shredded as soon as is possible. A designated secured file cabinet will be used exclusively for storing any paper PSWP.

(7) Generally, printing of identifiable PSWP will be discouraged but in such instance as such printing is necessary, the printing will be done using the Consortium-PSO’s designated printer. This printer will be used exclusively by the Consortium-PSO staff and will not be available to the Task Force staff except through the Consortium staff if the Task Force printer is malfunctioning.

(8) A minimum number of the Consortium-PSO staff and the Chair of the Mammography Measures Advisory Board and the Treatment Measures Advisory Board will have access to identifiable PSWP. Additional Consortium steering Committee members may if deemed necessary on a limited basis view identifiable PSWP provided they sign a confidentiality agreement for the sole purpose of providing advice to the Consortium staff regarding quality improvement and identifying quality deficits. The Task Force staff will not have access to this identifiable PSWP except for the Task Force Executive Director in her role as Director of the Consortium-PSO.

(i) the Consortium-PSO shall also protect media, whether in electronic, paper or other media or format, that contain PSWP by limiting access to authorized users, and sanitizing and destroying such media before their disposal or release for reuse; and

(ii) the Consortium-PSO shall also control and limit physical and virtual access to places and equipment where PSWP is received, accessed, or handled. This will be achieved by having the Consortium-PSO printer and PSWP file cabinet housed at the end of the offices next to the Consortium-PSO’s Associate Director.

(9) The IHA, on behalf of the Consortium-PSO, shall ensure that security controls and monitoring processes are in place, which address:

(i) identification of those authorized to receive, access, or handle PSWP electronically and an audit capacity to detect unlawful, unauthorized or inappropriate receipt, access or handling of PSWP; and

(ii) methods to prevent unauthorized receipt, access, or handling of PSWP.
(10) Only Consortium-PSO staff and the Chair of the Mammography Advisory Board and the Treatment Advisory Board will have access to identifiable PSWP. Additional members of the Consortium steering committee may have access to identifiable PSWP on a case by case basis provided they sign a confidentiality agreement. In addition, access may be granted to agents of the Consortium-PSO including, but not limited to, legal counsel, accountants, and outside medical consultants. Each of these individuals will be required to sign a confidentiality agreement stating that they will not disclose any identifiable PSWP. Inappropriate disclosure will be a dismissible offense under the confidentiality agreement.

(11) The Consortium-PSO shall periodically assess security risks and controls to establish if its controls are effective, to correct any deficiency identified and to reduce or eliminate any vulnerabilities.

(12) The Consortium-PSO shall assess its system and communications protection to monitor, control and protect the Consortium-PSO receipt, access or handling of PSWP with particular attention to the transmission of PSWP to and from participating healthcare providers, other PSOs, contractors or any other responsible persons.

(13) In general, aggregate de-identified data will be provided by participating healthcare providers to the Consortium-PSO and such data will not contain protected health information as defined by the HIPAA Privacy Rule. An exception to this general rule may be necessary for data matching for the City of Chicago for the purpose of determining follow-up care for women screened at the Chicago Department of Public Health (CDPH) but whose follow up care is provided by a facility other than a CDPH facility. In such instance, the Consortium-PSO will enter into a HIPAA business associate agreement with CDPH. Use of protected health information (PHI) will be exclusively for the purpose of data matching and the Consortium-PSO will ensure that measures are taken to minimize the risk of disclosure including timely destruction of PHI after its purpose has been accomplished. If in the future the Consortium-PSO does get access to protected health information, the Consortium-PSO shall enter into business associate agreements with participating healthcare providers in accordance with the requirements set forth in the HIPAA Privacy Rule to ensure the confidentiality and security of any PSWP. The Consortium-PSO shall comply with the provisions of its business associate agreements with respect to any disclosure of identifiable PSWP authorized herein. The individually identifiable patient information will remain at the provider’s site and will not be transmitted to the Consortium in individually identifiable form.