



# Washington State Health Information Infrastructure Advisory Board (HIIAB) Privacy, Security, and Confidentiality

## Criteria for Pilot Privacy and Security Assessment

Below are the proposed criteria for assessing the Health Record bank pilots. Several sources were used to develop the criteria, including but not limited to:

- Markle Foundation – This work was originally published as part of a compendium called [Connecting for Health Common Framework for Networked Personal Health Information](http://www.connectingforhealth.org/phti/index.html). The details of this work can be found at <http://www.connectingforhealth.org/phti/index.html>. It is copyrighted but is available to the public at no charge.
- Patient Privacy Certified, Inc. – This framework relates to the PPC privacy certification process and was provided to us for our consideration. The full certification is fee-based and requires a security audit in advance. Contact PPC's CEO, at [william.yasnoff@nhiiadvisors.com](mailto:william.yasnoff@nhiiadvisors.com) for details.
- John R. Christiansen, with Christiansen IT Law – This privacy and security assurance framework, and the principles within it were used to inform certain aspects of this assessment approach. John's website is located at <http://www.christiansenlaw.net/>.

The goal of the pilot assessment is to help the HCA better understand the approach and policies of the pilots in each of the key areas of security and privacy. Pilots will be assessed on how well they met their contract commitments to the HCA, namely the requirements established in the grant solicitation regarding security (requirement #7 on pages 6/7).

Additionally, the AccessMyHealth.Org project team will use the results of the assessment to ensure communication materials are accurate, and that patients and providers receive a clear description and full disclosure of each pilot's business practices.

The assessment criteria and the actual assessment results are not intended to serve as an endorsement or certification of the pilot's business practices. The assessment results will be shared with the HCA and other project staff as needed. Where feasible, Health Record Banks are encouraged to seek "certification" of the security and privacy practices.

## Security Assessment Criteria

Principle	Criteria	Comments and Additional Sources
<p>A. Authentication of Consumers and other individuals using the system. See Markle CT2 and Christiansen framework (see page 16, “level 3 procedures”).</p>	<p>A.1 All users and machines* that interact with the system have been thoroughly authenticated and documented. A.2 Authentication policy is in place and has high level of assurance (see level 3 in Christiansen framework, pg. 16, e.g. identify is vetted against government issued ID).</p>	<p>Authentication practices form the cornerstone of security and privacy.</p> <p>* Only machines that automatically provide clinical data to the HRB will be authenticated. Users can use any machine with a browser to access the HRB with a security code.</p>
<p>B. Binding Agreements are used for all parties and establish a chain of trust.</p> <p>See Christiansen framework (see page 8 on the factors for Business Agreements).</p>	<p>B.1 All agreements are in accordance with the privacy policies and other policies of the system. B.2 Organizations/individuals that serve to register individuals agree to register in accordance with authentication standards. B.3 Consumers execute binding usage agreements. B.4 Providers accessing the data execute binding agreements.</p>	<p>Evaluate basic agreements that are used.</p> <p>Use Christiansen (page 8) and Markle frameworks to review the contracts and provide feedback on basic elements contained.</p>
<p>C. Provision with ID and initiation code, out of band.</p> <p>Christiansen framework vaguely identifies this on page 7, “provisioning”.</p>	<p>C.1 Users are delivered a user name and code (initial password) to initiate the account. C.2 The information is provided either in person, via US mail or in a manner that cannot be intercepted.</p>	<p>Review process flow and basic procedures to ensure elements that lead to non-repudiation are in place and effective.</p> <p>Identify any inconsistencies and provide guidance.</p>

## Security Assessment Criteria Contd.

Principle	Criteria (references to PPC)	Comments and Additional Sources
<p>D. Policy Notice to Consumers.</p> <p>See Markle CP2 and PPC criteria</p>	<p>D.1 Patients have easy access to the written privacy policy and any related materials. (1.3, 1.10, 1.11)</p> <p>D.2 Policy is written in a manner that is easy to understand. (1.4, 1.5, 1.6, 1.7, 1.8, 1.9)</p> <p>D.3 Policy statement explicitly includes all related technology vendors and applies to all “downstream” companies that may have access to the information. (1.2, 2.2, 2.6, 2.8, 2.14)</p> <p>D.4 Policy and or related materials clearly describe who and when/how others may have access to the personal information. (1.2, 2.4, 2.6, 2.7, 2.8)</p> <p>D.5 Policy clearly binds other that may have access to the information. (2.14, 4.1, 4.2)</p>	<p>Transparency is a key to trust, policy should be clear, easily accessible and apply to all downstream entities.</p> <p>Determining if a policy is “easily understood” is subjective and requires the assessor to provide meaningful feedback and edits so that improvement ideas are actionable. Use of PPC specific criteria may be helpful in this regard.</p>
<p>E. Consumer Consent.</p> <p>See Markle CP3 and PPC criteria</p>	<p>E.1 Patients have clearly “opted in” to put their data into the HRB and any related applications. (3.1, 3.2)</p> <p>E.2 Patients clearly consent to the release of their data to specific individuals/organizations and or to role based situations if proper patient consent is communicated and subsequently obtained, including but not limited to any use or sales of the data in aggregate form. (2.8, 3.1, 4.1)</p>	<p>Tell consumers what you will and won’t do with their data, disclose all third parties involved.</p> <p>Consumers explicitly decide to be included in all uses of their data, even if in aggregated form.</p>
<p>F. Consumer Obtainment and Control</p> <p>See Markle CP8 and PPC criteria:</p>	<p>F.1 Patients are told what data they can control and any limitations that may exist. (1.1, 2.5, 13.4)</p> <p>F.2 Patients are told how their data may be accessed during an emergency and how such an emergency is later reviewed and they are notified. (7.6, 7.7, 2.6, 2.7, 2.10, 2.11, 10.1)</p> <p>F.3 Patient may choose to close their account and delete all records within a specified time. (3.3, 6.2)</p>	<p>Describe accurately to consumers the extent to which the employed technology let’s them control who sees what and to what degree of granularity</p>

## Security Assessment Criteria Contd.

Principle	Criteria (references to PPC)	Comments and Additional Sources
<p>G. Immutable Audit Trails.</p> <p>See Markle CT3 and PPC criteria.</p>	<p>G.1 Ensure audit trails are in place for all occurrences of data access, batch and real time. (9.1, 9.2, 9.3, 9.4, 9.5)</p> <p>G.2 Can audit trails be produced if requested by the patient? (9.7)</p> <p>G.3 Are audit trails immutable and secure? (9.6)</p> <p>G.4 Patients have ability to report concerns about privacy or security concerns.</p>	<p>Develop audit trails - a log of who-saw-what-info-when.</p>
<p>H. Limitations on Identifying Information.</p> <p>See Markle CT4 and PPC criteria:</p>	<p>H.1 Patients are told about profiling or tracking practices and the specific data used for this purpose is disclosed. (5.1, 5.2)</p>	<p>Understand and disclose the extent to which the pilots and their partners will be capturing electronic identifiers (not demographic) and what are risks of this activity, especially if the information is shared with other organizations.</p>

## Procedure for the Assessment

1. Bill Yasnoff, MD, PhD will interview and discuss the proposed approach, technologies, privacy policies, and business practices with each pilot and will use these criteria to guide his review and discussions.
2. Dr. Yasnoff will evaluate his findings and review them with Howard Thomas. Consultants will apply the basic assessment criteria, seek additional input and clarifications, and provide feedback to the pilots.
3. Consultants will complete their findings and recommendations and provide feedback to the HCA and the pilots.
4. The HCA will evaluate the assessment results, seek additional input, and provide direction based on the results.

For more information contact:

Juan Alaniz, Project Manager • [juan.alaniz@hca.wa.gov](mailto:juan.alaniz@hca.wa.gov) • (360) 923-2726