

**Privacy and Security Workgroup (PSWG)**

**Data Segmentation for Privacy (DS4P)**

**Comment on whether the PSWG agrees with ONC’s proposal; specifically, that DS4P send and receive technology should be part of the 2015 certification criteria, as described in the NPRM.**

| **2015 Edition Health IT Certification Criterion § 170.315(b)(7) (Data segmentation for privacy – send)**  **&**  **2015 Edition Health IT Certification Criterion § 170.315(b)(8) (Data segmentation for privacy – receive)** |
| --- |
| **§ 170.315(b)(7) (Data segmentation for privacy – send)**  pp. 16841 - 16842 of the FR Vol.80, No. 60:A provider currently cannot send sensitive patient information electronically without some technical capability to indicate information is subject to restrictions, such as a prohibition on re-disclosure without consent, consistent with 42 CFR Part 2. The sending provider also must have confidence that the receiver can properly handle electronically sent 42 CFR Part 2-covered data. Because neither of these functionalities are currently supported in certification, sensitive health information such as 42 CFR Part 2-covered data is often only shared via paper and fax. We propose, consistent with the HITPC recommendations, that for certification to this criterion, a Health IT Module must be able to send documents using document level tagging (Level 1) in accordance with the DS4P Implementation Guide (IG).  **§ 170.315(b)(8) (Data segmentation for privacy – receive)**  P. 16842: In general, 42 CFR Part 2-covered data is not currently provided electronically to healthcare providers through electronic exchange. Instead, the status quo remains to share 42 CFR Part 2-covered data via paper and fax. In line with the HITPC recommendations, we propose a certification criterion that would require a Health IT Module to be able to receive 42 CFR Part 2-covered data in accordance with the DS4P Implementation Guide (IG). DS4P at the document level (Level 1) of the recommendations allows recipient health IT to receive, recognize, and view documents with privacy metadata tagging indicating certain restrictions from 42 CFR Part 2 providers with the document sequestered from other health IT data. A recipient provider could use document level tagging to sequester the document from other documents received and help prevent unauthorized re-disclosure, while allowing the sensitive data to flow more freely to authorized recipients. Thus, consistent with the HITPC recommendations, we propose that a Health IT Module be able to receive documents tagged with privacy metadata tagging (Level 1). |

**Public Comment Field**:

The Privacy and Security Tiger Team (the predecessor to the Privacy and Security Workgroup (Workgroup)) previously recommended the inclusion of DS4P “send” and “receive” functionality as voluntary criteria for EHR certification. Although the Tiger Team recognized the important, initial step that DS4P Send and Receive takes toward enabling the exchange of sensitive health data protected by 42 CFR Part 2 (Part 2), the Tiger Team had significant concerns with the technology and numerous questions about how it could be implemented. Ultimately, the Tiger Team felt that offering the functionality as a “voluntary” part of the meaningful use certification program would enable those providers who wanted to take advantage of the technology to obtain it. The Team also raised questions about the maturity of DS4P, encouraged further pilots of the technology, and sought clarification of a number of policy issues that had arisen as part of the discussion. The Health IT Policy Committee endorsed these recommendations and forwarded them to ONC (available at: <http://healthit.gov/sites/faca/files/PSTT_DS4P_Transmittal%20Letter_2014-07-03.pdf>). The concerns expressed in the recommendation transmittal letter were not noted in the proposed certification rule.

In evaluating the proposed DS4P criteria for the next phase of certification, the Workgroup echoed some of the concerns initially expressed by the Tiger Team:

* The limitations of document level sequestration, with a read-only capability (information cannot be consumed/interdigitated in the EHR, including decision support software);
* Uncertainty about the extent to which the DS4P technology would enable compliance with Part 2 requirements after receipt of the segmented document;
* Policy uncertainties about whether a provider can manually enter similar data received directly from a patient, and whether that data, if subject to Part 2, would then be protected by DS4P Receive against subsequent re-disclosure without authorization (and the paradox of regulating this information differently based on its source);
* Uncertainty regarding whether DS4P Send and Receive is appropriate to enable compliance with other sensitive data laws that may not include prohibitions on re-disclosure;
* Discomfort among providers about “swiss cheese” electronic medical records (records that are incomplete when patients withhold information) in a digital environment where there are greater expectations for the completeness of electronic medical records (EMRs).

**Upon further review, the Workgroup has decided to leave to the Standards Committee the determination of whether DS4P Send and Receive are mature enough to be included in the 2015 EHR certification program.** (Of note, in the original recommendation letter, the Tiger Team and the Committee recognized the traditional and important role of the Standards Committee in determining whether standards and functionalities are mature enough to be part of ONC’s EHR certification program.)

Under the current NPRM proposal, out of band communication between providers about re-disclosure obligations may still be required. Because the proposed criteria are voluntary, a provider with DS4P Send functionality could send sensitive information to a provider who does not have the DS4P Receive functionality. Yet, the receiver without the technology would not be able to view the document-level security tag and may not be aware of the re-disclosure limitations associated with the document. Moreover, a DS4P Send provider may not know whether the receiving provider possesses DS4P Receive functionality. Therefore, to be compliant with law (especially Part 2), the sender may need to verify this offline with the receiving provider and potentially employ other means to communicate re-disclosure restriction information. The Workgroup further acknowledges that the lack of harmonization of state and federal laws on sensitive data, as outlined in the ONC Interoperability Roadmap (<http://www.healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf>) further compounds the problem. Variation in sensitive data laws makes it more complex to move forward with the development of technologies that enable compliance.

Related to the issue of maturity, the Workgroup discussed the more granular functionality of DS4P technology. Although the proposed criteria require a document-level tagging, more granular privacy tagging at the section and data element levels is currently technically possible. These capabilities have not been widely implemented or tested, especially around how the receiving system would need to implement the requirements to be consistent with applicable sensitive data laws.

The Workgroup agrees that the electronic exchange of sensitive information is critically important for the future of health IT, and DS4P Send-Receive lays an initial foundation for enabling those data flows. This technology should be available for those who seek to implement it. The Workgroup underscores the importance of **continuing to pilot and test in order to refine technologies that enable the sharing of sensitive data in compliance with law.** The Workgroup further recommends that ONC **educate providers and patients** about the features and limitations of the technology so that they can make intelligent decisions with respect to the adoption of DS4P functionality.

**Pharmacogenomics Data**

| **5. Pharmacogenomics Data – Request for Comment** |
| --- |
| pp. 16869 - 16870: Pharmacogenomics data identifies genetic variants in individuals that alter their metabolism or other interactions with medications and can lead to serious adverse events. This information is being included in an increasing number of FDA-approved drug labels. Health IT systems that can capture pharmacogenomics information could be used to increase patient safety and enhance patient outcomes. |
|  |

**Public Comment Field:**

The Workgroup acknowledges that the use of pharmacogenomics data will become an integral part of medicine in the future, but **the PSWG concludes that introducing certification for this functionality in the 2015 Edition is premature**. Some members questioned the current clinical usefulness of pharmacogenomics information due to the nascent state of the science, while other members cited current use cases in clinical practice and the potential benefit of being able to predict appropriate therapies. Members also highlighted the current lack of harmonization of state and federal laws regarding genetic and other sensitive information as another inhibitor to adoption. The Workgroup encourages ONC to continue to thoughtfully review issues around accessing, sharing, and using pharmacogenomics data as the science evolves.

On the question of whether health IT should be required to apply different rules for the use and exchange of genetic, genomic, or pharmacogenomics data, such as those related to behavioral health, the Workgroup strongly cautions ONC from promoting **policies that require higher or more complex protection than what is provided for in current law.** The Workgroup also does not agree that using DS4P is useful for providers in helping them to comply with more sensitive laws governing pharmacogenomics data; one key use of pharmacogenomics data is in safe prescribing, and DS4P does not enable the use of decision-support software due to its document-level segmentation approach.