

Written Testimony on Proposed HB 5737, to the Public Health Committee, February 27, 2013

Susan Israel, MD

I would like to thank the members of the Public Health Committee for this opportunity to speak on behalf of Proposed HB 5737 that will allow us to decide whether our health insurance companies can send our diagnoses, drugs taken, providers seen, procedures done, along with the dates, and our race and ethnicity into the centralized, All-Payer Claims Database, to be processed by a private company, with the data to be released by the State of CT. Hopefully, we will be the ones to decide how much risk to our privacy we wish to take, because there will be the inevitable hackers, breaches, and the re-identification of our data. It will also be the mother lode for identify theft. I believe that this bill would restore our Fourth Amendment rights to preserve our privacy.

It seems that *identified* data may be seen by people in State agencies and the CT Health Insurance Exchange who have signed agreements "consistent with the HIPAA rules regarding the safeguarding of Protected Health Information" which by HIPAA's definition is *identified* data, as de-identified data is no longer considered Protected Health Information (Sec. xx-xxx-5, d, p. 8 and Sec. xx-xxx-7, a, p. 8 of the APCD Regulations & HHS website on Health Information Privacy). The Administrator, appointed by the Governor, will have the power to determine who will see what of our data (Sec. xx-xxx 5, b). This will probably also allow the private vendor, as a business associate or covered entity, to see the identified data. If the data is identified, then will that part of the data that is classified by HIPAA as "Sensitive" such as psychiatric care, HIV status, STI's, etc., be handled with enhanced privacy provisions? I have tried to confirm these issues with people involved in the State's APCD but have not been answered.

The APCD regulations may be internally inconsistent as in one section (Sec. xx-xxx-4, b, p.6) it says that "The Administrator will make available to the public, standard, aggregated reports and data files containing information regarding utilization, cost and quality of services." However, in another Section (Sec. xx-xxx-5, c, 1, p. 7), it defines "Public Use Data Sets" as being only de-identified according to HIPAA rules (HHS website and 45 C.F.R. Section 164.514 b, 2, i & 45 C.F.R. 164.514 e, 2) which call for the removal of the patient and family names, their id numbers and address, except the state. The day and month, but not the year, of patient ages and medical services will be removed. CT will also remove the names of the providers and the insurance companies from the public data sets, but they will be given to certain groups along the patient's zip code, and it seems with the full dates of their age and services (Sec. xx-xxx-5, c, 2, p.8). These groups could find me with only my zip code as I live in a small town with one school, with one child of a certain age.

But if the data is released to the public in a de-identified form or if it is not carefully aggregated, then your neighbor could recognize you with what is left: such as the year of delivery of your children, that you have MS or were treated for a broken leg, and this would be possible without access to electronic health records and other data bases. You might say, so what if your dermatologist's staff could re-identify you from the released data as they already have your record, but they may not have known that you were treated with an antidepressant three years ago, or that you terminated a pregnancy or that you have been treated for ED.

## U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

### Health Information Privacy

<b>Health Information</b>	<p>Any information, whether oral or recorded in any form or medium, that:</p> <ul style="list-style-type: none"> <li>• (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and</li> <li>• (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.</li> </ul>
<b>Individually Identifiable Health Information</b>	<p>Information that is a subset of health information, including demographic information collected from an individual, and:</p> <ul style="list-style-type: none"> <li>(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and</li> <li>(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to the individual; and             <ul style="list-style-type: none"> <li>(i) That identifies the individual; or</li> <li>(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.</li> </ul> </li> </ul>
<b>Protected Health Information</b>	<p>Individually identifiable health information:</p> <ul style="list-style-type: none"> <li>(1) Except as provided in paragraph (2) of this definition, that is:             <ul style="list-style-type: none"> <li>(i) Transmitted by electronic media;</li> <li>(ii) Maintained in electronic media; or</li> <li>(iii) Transmitted or maintained in any other form or medium.</li> </ul> </li> <li>(2) Protected health information excludes individually identifiable health information in:             <ul style="list-style-type: none"> <li>(i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;</li> <li>(ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and</li> <li>(iii) Employment records held by a covered entity in its role as employer.</li> </ul> </li> </ul>
<b>Suppression</b>	<p>Withholding information in selected records from release.</p>

[Back to top](#)

1. The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA). Section 13424(c) of the HITECH Act requires the Secretary of HHS to issue guidance on how best to implement the requirements for the de-identification of health information contained in the Privacy Rule.

2. Protected health information (PHI) is defined as individually identifiable health information transmitted or maintained by a covered entity or its business associates in any form or medium (45 CFR 160.103). The definition exempts a small number of categories of individually identifiable health information, such as individually identifiable health information found in employment records held by a covered entity in its role as an employer.

3. Detailed definitions and explanations of these covered entities and their varying types can be found in the "Covered Entity Charts" available through the OCR website, at <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html>. Discussion of business associates can be found at <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html>.

4. In some instances, other federal protections also may apply, such as those found in Family Educational Rights and Privacy Act (FERPA) or the Common Rule.

5. Subcommittee on Disclosure Limitation Methodology, Federal Committee on Statistical Methodology. Report on statistical disclosure limitation methodology. *Statistical Policy Working Paper 22, Office of Management and Budget*. May 1994. Revised by the Confidentiality and Data Access Committee. 2005. Available online: [http://www.fcsm.gov/working-papers/SPWP22\\_rev.pdf](http://www.fcsm.gov/working-papers/SPWP22_rev.pdf)

6. This table was adapted from B. Malin, D. Karp, and R. Scheuermann. Technical and policy approaches to balancing patient privacy and data sharing in clinical and translational research. *Journal of Investigative Medicine*. 2010; 58(1): 11-18.

7. Supra note 3.

8. In general, it helps to separate the "features," or types of data, into classes of relatively "high" and "low" risks. Although risk actually is more of a continuum, this rough partition illustrates how context impacts risk.

9. See L. Sweeney. Testimony before that National Center for Vital and Health Statistics Workgroup for Secondary Uses of Health Information. August 23, 2007.

10. See P. Golle. Revisiting the uniqueness of simple demographics in the US population. In *Proceedings of the 5th ACM Workshop on Privacy in the Electronic Society*. ACM Press, New York, NY. 2006: 77-80.

11. See L. Sweeney. K-anonymity: a model for protecting privacy. *International Journal of Uncertainty, Fuzziness, and Knowledge-Based Systems*. 2002; 10(5): 557-570.

12. See K. Benitez and B. Malin. Evaluating re-identification risks with respect to the HIPAA Privacy Rule. *Journal of the American Medical Informatics Association*. 2010; 17(2): 169-177.

13. Figure based on Dan Barth-Jones's presentation, "Statistical de-identification: challenges and solutions" from the Workshop on the HIPAA Privacy Rule's De-Identification Standard, which was held March 8-9, 2010 in Washington, DC.

# U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

## Health Information Privacy

- the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Protected health information includes many common identifiers (e.g., name, address, birth date, Social Security Number) when they can be associated with the health information listed above.

For example, a medical record, laboratory report, or hospital bill would be PHI because each document would contain a patient's name and/or other identifying information associated with the health data content.

By contrast, a health plan report that only noted the average age of health plan members was 45 years would not be PHI because that information, although developed by aggregating information from individual plan member records, does not identify any individual plan members and there is no reasonable basis to believe that it could be used to identify an individual.

The relationship with health information is fundamental. Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data (see above). If such information was listed with health condition, health care provision or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.

[Back to top](#)

## Covered Entities, Business Associates, and PHI

In general, the protections of the Privacy Rule apply to information held by covered entities and their business associates. HIPAA defines a covered entity as 1) a health care provider that conducts certain standard administrative and financial transactions in electronic form; 2) a health care clearinghouse; or 3) a health plan. A business associate is a person or entity (other than a member of the covered entity's workforce) that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of protected health information. A covered entity may use a business associate to de-identify PHI on its behalf only to the extent such activity is authorized by their business associate agreement.

See the OCR website <http://www.hhs.gov/ocr/privacy/> for detailed information about the Privacy Rule and how it protects the privacy of health information.

[Back to top](#)

## De-identification and its Rationale

The increasing adoption of health information technologies in the United States accelerates their potential to facilitate beneficial studies that combine large, complex data sets from multiple sources. The process of de-identification, by which identifiers are removed from the health information, mitigates privacy risks to individuals and thereby supports the secondary use of data for comparative effectiveness studies, policy assessment, life sciences research, and other endeavors.

The Privacy Rule was designed to protect individually identifiable health information through permitting only certain uses and disclosures of PHI provided by the Rule, or as authorized by the individual subject of the information. However, in recognition of the potential utility of health information even when it is not individually identifiable, §164.502(d) of the Privacy Rule permits a covered entity or its business associate to create information that is not individually identifiable by following the de-identification standard and implementation specifications in §164.514(a)-(b). These provisions allow the entity to use and disclose information that neither identifies nor provides a reasonable basis to identify an individual. As discussed below, the Privacy Rule provides two de-identification methods: 1) a formal determination by a qualified expert; or 2) the removal of specified individual identifiers as well as absence of actual knowledge by the covered entity that the remaining information could be used alone or in combination with other information to identify the individual.

Both methods, even when properly applied, yield de-identified data that retains some risk of identification. Although the risk is very small, it is not zero, and there is a possibility that de-identified data could be linked back to the identity of the patient to which it corresponds.

Regardless of the method by which de-identification is achieved, the Privacy Rule does not restrict the use or disclosure of de-identified health information, as it is no longer considered protected health information.

[Back to top](#)

## The De-identification Standard

Section 164.514(a) of the HIPAA Privacy Rule provides the standard for de-identification of protected health information. Under this standard, health information is not individually identifiable if it does not identify an individual and if the covered entity has no reasonable basis to believe it can be used to identify an individual.

**§ 164.514 Other requirements relating to uses and disclosures of protected health information.**

(a) *Standard: de-identification of protected health information.* Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

## U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

### Health Information Privacy

Sections 164.514(b) and (c) of the Privacy Rule contain the implementation specifications that a covered entity must follow to meet the de-identification standard. As summarized in Figure 1, the Privacy Rule provides two methods by which health information can be designated as de-identified.

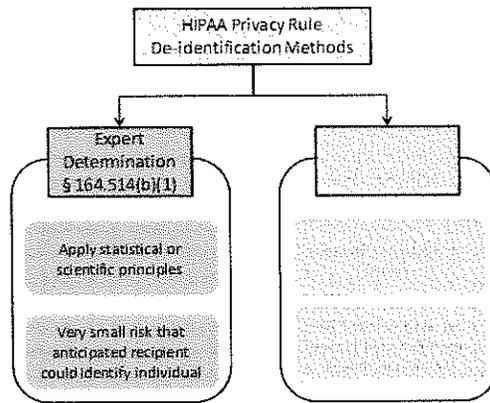


Figure 1. Two methods to achieve de-identification in accordance with the HIPAA Privacy Rule.

The first is the "Expert Determination" method:

(b) *Implementation specifications: requirements for de-identification of protected health information.* A covered entity may determine that health information is not individually identifiable health information only if:

(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

(ii) Documents the methods and results of the analysis that justify such determination; or

The second is the "Safe Harbor" method:

(2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

(A) Names	
(B) All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census:	
(1) The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and	
(2) The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000	
(C) All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older	
(D) Telephone numbers	(L) Vehicle identifiers and serial numbers, including license plate numbers
(E) Fax numbers	(M) Device identifiers and serial numbers
(F) Email addresses	(N) Web Universal Resource Locators (URLs)
(G) Social security numbers	(O) Internet Protocol (IP) addresses
(H) Medical record numbers	(P) Biometric identifiers, including finger and voice prints
(I) Health plan beneficiary numbers	(Q) Full-face photographs and any comparable images
(J) Account numbers	(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section [Paragraph (c) is presented below in the section "Re-identification"]; and
(K) Certificate/license numbers	

R-39 Rev. 03/2012  
(Title page)

**IMPORTANT:** Read instructions on back of last page (Certification Page) before completing this form. Failure to comply with instructions may cause disapproval of proposed Regulations

State of Connecticut  
**REGULATION**  
of

---

NAME OF AGENCY

Office of Policy and Management

---

**Concerning**

---

SUBJECT MATTER OF REGULATION

All-Payer Claims Database

---

**All-Payer Claims Database.**

Sec. 1. The Regulations of Connecticut State Agencies are amended by adding Section xx-xxx-1 to xx-xxx-7, inclusive, as follows:

**(NEW) Section xx-xxx-1: Definitions.**

As used in sections xx-xxx-2 to xx-xxx-7, inclusive, of the Regulations of Connecticut State Agencies:

- (1) "Administrator" means the Special Advisor to the Governor on Healthcare Reform or his or her designee.
- (2) "APCD" means the Connecticut All Payer Claims Database as established under Public Act 12-166.
- (3) "Day" means a calendar day.
- (4) "Dental Claims Data File" means a data file composed of service level remittance information including, but not limited to, member demographics, provider information, charge and payment information, and current dental terminology codes from all Member paid claims and encounters.
- (5) "Eligibility Data File" means a data file composed of demographic information for each Member who is eligible to receive medical, pharmacy, or dental coverage provided or administered by a Reporting Entity for one or more days of coverage during the reporting month.
- (6) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d – 1320d-8, and its implementing regulations, including 45 C.F.R. Parts 160, 162 and 164, as amended from time to time.
- (7) "Historic Data" means Eligibility Data File(s), Medical Claims Data File(s), Pharmacy Claims Data File(s) and Provider File(s) for the period commencing January 1, 2010 through December 31, 2012, or such later three year period specified by the Administrator.
- (8) "Medical Claims Data File" means a data file composed of service level remittance information including, but not limited to, member demographics, provider information, charge and payment information, and clinical diagnosis/procedure codes from all paid claims and encounters.

- (9) "Member" means: (A) a Connecticut resident or (B) an individual who resides elsewhere but is covered under a Small Group Health Plan issued in Connecticut and purchased through the Connecticut Health Insurance Exchange, including the subscriber and any spouse or dependent, for whom a Reporting Entity adjudicates claims.
- (10) "Pharmacy Claims Data File" means a data file composed of service level remittance information including, but not limited to, member demographics, provider information, charge and payment information and national drug codes from all paid claims for each prescription filled.
- (11) "Provider File" means a data file that includes additional information, as specified in section xx-xxx-2 (b) (4) of the Regulations of Connecticut State Agencies, about the health care providers that are included in a Medical Claims Data File or Dental Claims Data File.
- (12) "Reporting Entity" has the same meaning as provided in Section 19a-724(a) (2) (B) of the 2012 Supplement to the General Statutes.
- (13) "Small Group Health Plan" means a health plan issued to a small employer as defined in Section 38a-564 of the Connecticut General Statutes.
- (14) "Submission Guide" means the document published by the Administrator that sets forth the data elements, formats, minimum thresholds and other specifications for Reporting Entities' submission of Eligibility Data Files, Medical Claims Data Files, Dental Claims Data Files, Pharmacy Claims Data Files, and Provider Files to the Administrator or his/her designee.
- (15) "Subscriber" is the individual eligible for coverage under an insured or self-funded health plan.

**(NEW) Section xx-xxx-2: Reporting Requirements.**

**(a) General.**

- (1) Each Reporting Entity shall submit complete and accurate Eligibility Data Files, Medical Claims Data Files, Pharmacy Claims Data Files, Dental Claims Data Files, and Provider Files to the Administrator or his/her designee for all of their Members in accordance with the Submission Guide and the requirements of this section. Each Reporting Entity shall also submit all Medical Claims Data Files, Dental Claims Data Files, Pharmacy Claims Data Files, and associated Provider Files for any claims processed by any sub-contractor on the Reporting Entity's behalf.
- (2) Reporting Entities that are in a contractor/subcontractor arrangement with each other and Reporting Entities that perform certain components of the claims adjudication process for the same Members under a shared services arrangement shall coordinate with each other to avoid duplicative submissions. Any Reporting Entity that administers claims of Members as a subcontractor of another Reporting Entity or can otherwise demonstrate that its submission of data regarding certain Members would result in a duplicative submission may request the Administrator to waive its obligation to submit data files for such Members as part of the annual registration process described in subsection (f) of this section.

**(b) Minimum Data Elements.**

- (1) Each Eligibility Data File shall contain (A) demographic information about the Member, including but not limited to, name, unique Member identifier (including Social Security Number when available), gender, date of birth, and race and ethnicity, (B) coverage information, including, but not limited to, payer name, plan ID, type of coverage, and year and month of eligibility, and (C) relevant provider-related information specified by the Administrator which may include, but is not limited to, the Member's primary care clinician and information about the Member's association with an Accountable Care Organization or similar organization.
- (2) Each Medical Claims Data File shall contain information regarding each claim, including, but not limited to (A) demographic information about the Member, including but not limited to, name, unique Member identifier (including Social Security Number when available), gender, and date of birth, (B) coverage information, including, but not limited to, payer name, plan ID, and type of coverage, and (C) information about the claim, including but not limited to, when the service was provided, diagnosis information, procedure codes, payment information (including amount charged, amount paid by the plan, and Member responsibility) and provider information.
- (3) Each Pharmacy Claims Data File shall contain information regarding each claim, such as (A) demographic information about the Member, including, but not limited to, name, unique Member identifier (including Social Security Number when available), gender, and date of birth, (B) coverage information, including, but not limited to, payer name, plan ID, and type of coverage, and (C) information about the claim, including but not limited to, information about the prescription filled, such as the drug name and code, quantity and day's supply, payment information (including amount charged, amount paid by the plan and Member responsibility), and provider information.
- (4) Each Provider File shall contain information about the provider, including, but not limited to, name, address information, identification numbers, and specialty codes.
- (5) Each Dental Claims Data File shall contain information regarding each claim, including, but not limited to (A) demographic information about the Member, including but not limited to, name, unique Member identifier (including Social Security Number when available), gender, and date of birth, (B) coverage information, including, but not limited to, payer name, plan ID, and type of coverage, and (C) information about the claim, including but not limited to, when the service was provided; diagnosis information; procedure codes; codes specific to dental services such as tooth number, surface code or tooth surface, and dental quadrant; payment information (including amount charged, amount paid by the plan and Member responsibility); and provider information. As an alternative to requiring the submission of a separate Dental Claims Data File, the Administrator may require that specific dental-related elements be added to the Medical Claims Data File, such as tooth number, surface code or tooth surface, and dental quadrant.

(c) **Reporting Schedule.**

(1) **Medical Claims Data and Pharmacy Claims Data.**

- (A) **Test Files.** Reporting Entities shall submit a test file of Eligibility Data, Medical Claims Data and Pharmacy Claims Data and associated Provider Files for a consecutive twelve month period to the Administrator or his/her designee on a date specified by the Administrator. The Administrator shall provide notice to Reporting Entities of the due date for the test file by written notice published on the website of the Office of Health Reform and Innovation, which due date shall in no event be less than 150 days after the issuance of the final Submission Guide.

- (B) **Historic Data.** Reporting Entities shall submit complete and accurate Historic Data that conforms to Submission Guide requirements to the Administrator no later than 90 days after the due date for the test file specified in subparagraph (A) of this subdivision.
- (C) **Year-to-date Data.** Reporting Entities shall submit complete and accurate Eligibility Data Files, Medical Claims Data Files, Pharmacy Claims Data Files and Provider Files covering the period from January 1, 2013, or such later date specified by the Administrator, through a date to be specified by the Administrator, by no later than 45 days after the due date for Historic Data specified in subparagraph (B) of this subdivision.
- (D) **Monthly Reporting.** On a monthly basis thereafter, Reporting Entities shall submit complete and accurate monthly Eligibility Data Files, Medical Claims Data Files, Pharmacy Claims Data Files, and Provider Files to the Administrator. Monthly files shall be submitted no later than the last day of the month following the end of the reporting month.
- (E) **Extensions.** Any request for an extension of time by a Reporting Entity shall be submitted to the Administrator in writing at least 45 days prior to the established deadline. The Administrator may consider requests submitted after that date in situations where the Reporting Entity subsequently discovers a technical problem that was not reasonably foreseeable on the date the extension request would otherwise have been due. The Administrator shall provide a written response to all requests for extensions.

(2) **Dental Claims Data.**

The Administrator shall establish a similar schedule for the reporting of Dental Claims Data by Reporting Entities, provided said schedule and detailed reporting specifications shall be incorporated into the Submission Guide. Notification of such changes shall be provided to Reporting Entities in accordance with subsection (e) of this section.

- (d) **Waivers of Data Submission Requirements.** The Administrator may waive data submission requirements for Reporting Entities that demonstrate to the Administrator's satisfaction that the required data elements are not available in the Reporting Entity's systems, or for Historic Data, if the Reporting Entity is not required to file data as of the effective date of these regulations due to insufficient enrollment as determined under subdivision (2) of subsection (g) of this section. As a condition for granting a waiver, the Administrator may require a Reporting Entity to submit a plan for improving conformance to data submission requirements. An approved waiver shall:
- (1) specify the data elements or files to which the waiver applies;
  - (2) specify the timeline for improved compliance, as applicable;
  - (3) identify the reason for the waiver; and
  - (4) specify the duration of the waiver, provided that all waivers shall expire at the end of the calendar year, unless the waiver explicitly states otherwise.

(e) **Submission Guide.**

- (1) The Administrator will produce and publish the Submission Guide to provide instructions to Reporting Entities on data elements, formats, minimum thresholds and other specifications for the Eligibility Data Files, Medical Claims Data Files, Dental Claims Data Files, Pharmacy Claims Data Files, and Provider Files to be submitted by Reporting Entities. The Administrator will publish the proposed Submission Guide on the website of the Office of Health Reform and Innovation. Reporting Entities and any other member of the public will be allowed to submit written comments to the Administrator concerning the proposed Submission Guide for thirty (30) days after the notice on the Office's website. The Administrator may, at his/her discretion hold a public hearing regarding the proposed Submission Guide. The Administrator will publish the final Submission Guide on such website. Thereafter the Administrator may amend the Submission Guide as necessary.

- (2) Prior to making any material revision to the Submission Guide, the Administrator will provide electronic notice of such proposal to all Reporting Entities that are registered and publish the proposed revisions on the website of the Office of Health Reform and Innovation. Reporting Entities and any other member of the public will be allowed to submit written comments to the Administrator concerning such proposed revisions for thirty (30) days after the notice on the Office's website. The Administrator may, at his or her discretion, hold a public hearing concerning proposed revisions to the Submission Guide. The Administrator will publish the final revisions on such website. Any such revisions shall not be effective until 180 days following publication of the final revisions on the website of the Office of Health Reform and Innovation.
- (3) The Administrator also may issue technical bulletins to clarify aspects of these regulations or the Submission Guide, provided that such technical bulletins will be published online on the website of the Office of Health Reform and Innovation. The Administrator will also provide electronic notice of any such revisions to all registered Reporting Entities. The Administrator may immediately implement technical or conforming revisions to the Submission Guide, upon provision of such notice.
- (f) **Annual Registration.** Beginning October 1, 2013, and annually thereafter, each Reporting Entity shall register with the Administrator on a form designated by the Administrator. The registration form shall indicate if the Reporting Entity is adjudicating claims for Members and, if applicable, the types of coverage, and its current enrollment. Reporting Entities may also request waivers of data submission requirements as part of the annual registration process.
- (g) **Exclusions.**
- (1) Claims related to the following types of policies shall be excluded from the files submitted by Reporting Entities: hospital confinement indemnity coverage; disability income protection coverage; accident only coverage; long term care coverage; specified accident coverage; Medicare supplement coverage; specified disease coverage; TriCare Supplemental Coverage; travel health coverage; and single service ancillary coverage, with the exception of dental and prescription drug coverage.
  - (2) Reporting Entities that, as of October 1<sup>st</sup> of any calendar year, have less than a total of 3,000 Members enrolled in plans that are offered or administered by the Reporting Entity are exempt from the data submission requirements set forth in subsections (a) to (c) of this section for the following calendar year. However, all Reporting Entities shall comply with the annual registration requirements contained in subsection (f) of this section.

**(NEW) Section xx-xxx-3: Non-Compliance and Penalties.**

- (a) Except where a waiver has been granted by the Administrator pursuant to Section xx-xxx-2(d), a Reporting Entity that fails to submit required data to the APCD in accordance with section xx-xxx-2 of the Regulations of Connecticut State Agencies, or fails to correct submissions rejected because of errors, shall be deemed a non-compliant Reporting Entity. If the Administrator finds that a Reporting Entity is non-compliant, the Administrator will provide written notice to the non-compliant Reporting Entity describing the deficiency. The non-compliant Reporting Entity shall provide the required information, or otherwise correct the deficiency, within thirty (30) days following receipt of said written notice.
- (b) If a non-compliant Reporting Entity does not provide the required information or correct the deficiencies within thirty (30) days, the Administrator may issue a notice of civil penalty to the non-compliant Reporting Entity. Such notice shall describe with specificity each failure on the part of the non-compliant Reporting Entity to provide data in accordance with section xx-xxx-2

of the Regulations of Connecticut State Agencies, the date that non-compliance began, and the per day civil penalty amount to be imposed. The Administrator may impose a civil penalty up to \$1,000 per day for each day the Reporting Entity is not in compliance.

- (c) Not later than fifteen days after receipt of the notice described in subsection (b) of this section, the non-compliant Reporting Entity may respond in writing to the Administrator detailing its efforts to comply with the relevant data submission requirements and any other facts the non-compliant Reporting Entity deems relevant to mitigate the civil penalty imposed.
- (d) Not later than fifteen days after the time for the non-complaint Reporting Entity to respond has expired, the Administrator shall issue a final notice of civil penalty. In addition to the items detailed in subsection (b) of this section, the final notice of civil penalty shall address the issues raised in the Reporting Entity's reply and, if applicable, detail the reasons for the Administrator's decision to reduce the amount of the civil penalty initially imposed. The final notice of civil penalty shall constitute a final decision by the Administrator for purposes of appeal to the Superior Court pursuant to 4-183 of the Connecticut General Statutes.

✓ (NEW) **Section xx-xxx-4: Data Utilization and Disclosure.**

- (a) The Administrator will utilize data in the APCD to provide health care consumers in the state with information through a web-based portal concerning the cost and quality of health care services that will allow such consumers to make economically sound and informed health care decisions.
- (b) The Administrator will make available to the public standard, aggregated reports and data files containing information regarding utilization, cost and quality of services.
- (c) The Administrator may provide custom data sets and reports to health care consumers and public and private entities engaged in reviewing health care utilization, cost, or quality of health care services, including community and public health assessment activities, subject to the procedures contained in xx-xxx-5 of the Regulations of Connecticut State Agencies and the limitations and conditions thereunder.

(NEW) **Section xx-xxx-5: Procedures for the Approval and Release of Claims Data.**

- (a) **Applications for Custom Data Sets.** An individual or entity seeking to obtain a custom data set containing data elements collected or generated by the Administrator or the Administrator's designee must submit a written application to the Administrator on a form prescribed by the Administrator.
  - (1) Such application shall include:
    - (A) a description of the data elements requested;
    - (B) the purpose of the project;
    - (C) a description of the research design and methodology; provided the applicant shall not be required to disclose proprietary methods, algorithms, tools, software programming or other similar non-public proprietary information.
    - (D) the procedures that will be used to maintain the confidentiality of any data provided; and
    - (E) a certification that the requestor will execute a data use agreement in the form prescribed by the Administrator restricting the use and disclosure of the data.
  - (2) The Administrator may tailor the type and level of information required in the application depending on whether the data set requested is a public use data set as described in subsection (c) (1) of this section, a limited data set as described in subsection (c) (2) of this section, or a data set described in subsection (c)(3) of this section.

- (3) The Administrator will post applications on the website of the Office of Health Reform and Innovation. The Administrator will not post those portions of applications that specify security measures or applications from law enforcement entities to the extent that posting the application on the website may impede the investigatory process. The Administrator will invite public comments on applications for at least ten (10) business days following the day on which the application is posted on the website. The Administrator will consider any comments received in conducting his or her review of an application.
- (4) The Administrator may approve an application if the Administrator determines that the request for data is consistent with the statutory purpose of the APCD, the applicant has demonstrated it is qualified to undertake the research or accomplish the intended use, the applicant requires such data in order to undertake the research or accomplish the intended use and the applicant can ensure the confidentiality and security of the data will be maintained. The Administrator shall provide a written response to each application, provided that any denial shall include the reasons for the decision. The Administrator's decision to approve or deny an application shall be final and shall not be subject to further review or appeal; provided nothing shall preclude an applicant whose application is denied from submitting a revised application for further consideration.

(b) **Data Release Advisory Committee.** The Administrator shall consult with a data release advisory committee in deciding whether to approve an application for a limited data set or an IRB-approved research study data set, and may also consult with the committee regarding applications for custom public use data sets. The data release review committee shall be comprised of members appointed by the Administrator and, at a minimum, shall include:

- (1) At least one member representing health insurers;
- (2) At least one member representing health care facilities;
- (3) At least one member representing a physician organization;
- (4) At least one member representing health care consumers;
- (5) At least one member representing employers;
- (6) At least one member representing health care researchers;
- (7) At least one member representing the state Medical Assistance Program; and
- (8) At least one member representing a pharmacy organization.

The Administrator may also consult with the committee on policies regarding the release and protection of data. The advice of the committee shall not be binding on the Administrator.

(c) **Public Use Data Sets, Limited Data Sets, and Institutional Review Board (IRB)-Approved Research Study Data Sets.** The Administrator may provide data to requestors at the following level of detail consistent with HIPAA rules regarding the safeguarding of Protected Health Information and the de-identification of data, and in compliance with state confidentiality requirements.

- (1) Public use data sets do not contain any identifiers listed in 45 C.F.R. Section 164.514(b)(2)(i), which listed identifiers include, but are not limited to, name and Social Security Number. Public use data sets also do not contain payer or individual health care professional names.

- (2) Limited data sets may contain: (A) date information and city and zip code information related to the Member, consistent with 45 C.F.R. 164.514(e)(2), and (B) payer and individual health care professional names with sufficient justification.
- (3) Consistent with HIPAA rules, full identifiers may be included in data sets provided to researchers or others with the duly authorized consent of the individuals whose identifiers as collected by the APCD would be included.
- (d) **Data to State Agencies and Connecticut Health Insurance Exchange.** The Administrator will provide data to Connecticut state agencies and the Connecticut Health Insurance Exchange for projects relating to the review of health care utilization, cost or quality of health care services, including for planning and carrying out of health improvement activities, upon the submission of a data management plan containing appropriate safeguards to maintain the confidentiality and security of the data and the signing of an appropriate data use or business associate agreement consistent with HIPAA rules regarding the safeguarding of Protected Health Information and the use of data use and business associate agreements.
- (e) **Means of Providing Data.** Data may be provided to approved applicants through secure file transfers and other electronic methods that protect the data from unauthorized access and disclosure, such as web-based query tools with customized, user-based access.

**(NEW) Section xx-xxx-6: Fees.**

The Administrator may charge a fee for data sets and reports.

**(New) Section xx-xxx-7: Privacy and Confidentiality.**

- (a) The Administrator may make data from the APCD available to public and private entities in accordance with section xx-xxx-5 when disclosed in a form and manner that is consistent with HIPAA rules regarding the safeguarding of Protected Health Information and the de-identification of data, and in compliance with state confidentiality requirements as well as state data security and confidentiality policies.
- (b) The Administrator shall institute appropriate administrative, physical and technical safeguards consistent with the HIPAA security rules contained in 45 C.F.R. Part 160 and Part 164, Subparts A and C, to ensure that data received from Reporting Entities is securely collected, compiled and stored.

**Statement of Purpose**

*Pursuant to CGS Section 4-170(b)(3), "Each proposed regulation shall have a statement of its purpose following the final section of the regulation." Enter the statement here.*

This proposed new regulation adopts rules for the operation of the all- payer claims data base program established under Public Act 12-166, including the reporting requirements for entities that are required to submit data, penalties for non-compliance, permitted uses of the data, procedures for the approval and release of data, collection of fees for data, and privacy and confidentiality requirements.

R-39 Rev. 03/2012  
(Certification page—see Instructions on back)

### CERTIFICATION

This certification statement must be completed in full, including items 3 and 4, if they are applicable.

- 1) I hereby certify that the above (check one)  Regulations  Emergency Regulations
- 2) are (check all that apply)  adopted  amended  repealed by this agency pursuant to the following authority(ies): (complete all that apply)
  - a. Connecticut General Statutes section(s) \_\_\_\_\_.
  - b. Public Act Number(s) 12-166.  
(Provide public act number(s) if the act has not yet been codified in the Connecticut General Statutes.)
- 3) And I further certify that notice of intent to adopt, amend or repeal said regulations was published in the **Connecticut Law Journal** on October 30, 2012;  
(Insert date of notice publication if publication was required by CGS Section 4-168.)
- 4) And that a public hearing regarding the proposed regulations was held on November 19, 2012;  
(Insert date(s) of public hearing(s) held pursuant to CGS Section 4-168(a)(7), if any, or pursuant to other applicable statute.)
- 5) And that said regulations are **EFFECTIVE** (check one, and complete as applicable)
  - When filed with the Secretary of the State
  - OR  on (insert date) \_\_\_\_\_

DATE	SIGNED (Head of Board, Agency or Commission)	OFFICIAL TITLE, DULY AUTHORIZED
------	--	---------------------------------

**APPROVED by the Attorney General as to legal sufficiency in accordance with CGS Section 4-169, as amended**

DATE	SIGNED (Attorney General or AG's designated representative)	OFFICIAL TITLE, DULY AUTHORIZED
------	---	---------------------------------

*Proposed regulations are **DEEMED APPROVED** by the Attorney General in accordance with CGS Section 4-169, as amended, if the attorney General fails to give notice to the agency of any legal insufficiency within thirty (30) days of the receipt of the proposed regulation.*

*(For Regulation Review Committee Use ONLY)*

- Approved  Rejected without prejudice
- Approved with technical corrections  Disapproved in part, (Indicate Section Numbers disapproved only)
- Deemed approved pursuant to CGS Section 4-170(c)

By the Legislative Regulation Review Committee in accordance with CGS Section 4-170, as amended	DATE	SIGNED (Administrator, Legislative Regulation Review Committee)
---	------	---

**Two certified copies received and filed and one such copy forwarded to the Commission on Official Legal Publications in accordance with CGS Section 4-172, as amended.**

DATE	SIGNED (Secretary of the State)	BY
------	---------------------------------	----

*(For Secretary of the State Use ONLY)*

**GENERAL INSTRUCTIONS**

1. All regulations proposed for adoption, amendment or repeal, *except* emergency regulations, must be presented to the Attorney General for his/her determination of legal sufficiency. (See CGS Section 4-169.)
2. After approval by the Attorney General, the original and one electronic copy (in Word format) of all regulations proposed for adoption, amendment or repeal must be presented to the Legislative Regulation Review Committee for its action. (See CGS Sections 4-168 and 4-170 as amended by Public Act 11-150, Sections 18 and 19.)
3. Each proposed regulation section must include the appropriate regulation section number and a section heading. (See CGS Section 4-172.)
4. New language added to an existing regulation must be in underlining or CAPITAL LETTERS, as determined by the Regulation Review Committee. (See CGS 4-170(b).)
5. Existing language to be deleted must be enclosed in brackets [ ]. (See CGS 4-170(b).)
6. A completely new regulation or a new section of an existing regulation must be preceded by the word "(NEW)" in capital letters. (See CGS Section 4-170(b).)
7. The proposed regulation must have a statement of its purpose following the final section of the regulation. (See CGS Section 4-170(b).)
8. The Certification Statement portion of the form must be completed, including all applicable information regarding *Connecticut Law Journal* notice publication date(s) and public hearing(s). (See more specific instructions below.)
9. Additional information regarding rules and procedures of the Legislative Regulation Review Committee can be found on the Committee's web site: <http://www.cga.ct.gov/lrr/>.
10. A copy of the Legislative Commissioners' Regulations Drafting Manual is located on the LCO website at [http://www.cga.ct.gov/lco/pdfs/Regulations\\_Drafting\\_Manual.pdf](http://www.cga.ct.gov/lco/pdfs/Regulations_Drafting_Manual.pdf).

**CERTIFICATION STATEMENT INSTRUCTIONS**

(Numbers below correspond to the numbered sections of the statement)

1. Indicate whether the regulation is a regular or an emergency regulation adopted under the provisions of CGS Section 4-168(f).
2.
  - a) Indicate whether the regulations contains newly adopted sections, amendments to existing sections, and/or repeals existing sections. Check all cases that apply.
  - b) Indicate the specific legal authority that authorizes or requires adoption, amendment or repeal of the regulation. If the relevant public act has been codified in the most current biennial edition of the *Connecticut General Statutes*, indicate the relevant statute number(s) instead of the public act number. If the public act has not yet been codified, indicate the relevant public act number.
3. Except for emergency regulations adopted under CGS 4-168(f), and technical amendments to an existing regulation adopted under CGS 4-168(g), an agency must publish notice of its intent to adopt a regulation in the *Connecticut Law Journal*. Enter the date of notice publication.
4. CGS Section 4-168(a)(7) prescribes requirements for the holding of an agency public hearing regarding proposed regulations. Enter the date(s) of the hearing(s) held under that section, if any; also enter the date(s) of any hearing(s) the agency was required to hold under the provisions of any other law.
5. As applicable, enter the effective date of the regulation here, or indicate that it is effective upon filing with the Secretary of the State. Please note the information below.

Regulations are effective upon filing with the Secretary of the State or at a later specified date. See CGS Section 4-172(b) which provides that each regulation is effective upon filing, or, if a later date is required by statute or specified in the regulation, the later date is the effective date. An effective date may not precede the effective date of the public act requiring or permitting the regulation. Emergency regulations are effective immediately upon filing with the Secretary of the State, or at a stated date less than twenty days thereafter.