PUBLIC COMMENTS

On behalf of UnitedHealthcare and its affiliated companies, hereinafter referred to as UnitedHealth Group, we appreciate the opportunity to comment on the proposed Access Health CT APCD Privacy Policy and Procedure.
Our specific concerns regarding data release are outlined below.

Confidential and Proprietary Information
The information submitted to the APCD contains certain financial information that Data Submitters consider to be confidential and proprietary in nature, often containing information that amounts to trade secrets. If this financial information is inappropriately released or disclosed by the APCD, it may cause harm to the marketplace by reducing competition, which may result in increased prices, or reduced quality and availability of health care services. It is important that Access Health CT recognize that financial data and information held by the APCD is confidential and proprietary, amounting to trade secrets, and take the steps necessary to ensure that such information is protected when re-released to the public by Access Health CT. The Federal Government recognizes the critical importance of protecting financial data/information when supplied by a group of payers and regulates this activity in the Department of Justice and Federal Trade Commission's Statement of Antitrust Enforcement Policy in Health Care – Statement 6. Statement 6 outlines appropriate safeguards and protections that should be in place in order to ensure that the exchange or release of confidential and propriety information does not facilitate collusion or anti-competitive behaviors, thereby reducing competition and increasing prices and availability of health care services. Due to the confidential and proprietary nature of the financial information submitted by Data Submitters, we request that in the development of the APCD's data release program and policies that you include language that protects payers' confidential and proprietary financial information.

We request that Section 12. Confidentiality. of the proposed APCD Privacy Policy and Procedure be revised to include a reference to the Department of Justice and Federal Trade Commission Statement referenced above and clearly state that payers' propriety and confidential financial information re-released to the public will be fully protected by Access Health CT – even treated as a State trade secret.

Data Release Comment Period
In order to further the goals of transparency and to allow for the review of data in accordance with state and federal law as outlined in Connecticut General Statute Section 38a-1091, we encourage Access Health CT to consider the implementation of a data release review process similar to those that have been implemented in its sister-APCDs in both Massachusetts and Maine, both of which allow for public comment to proposed data releases. We would like to propose the following process: the Executive Director will post a notice of data release application on the Access Health CT website. The Executive Director should include, at a minimum, the level of data being requested and the proposed purpose for which the request is being made. The Executive Director should invite public comments on applications for at least ten (10) business days following the day on which the application is posted on the website. After the public comment period ends, if the Executive Director determines that: (a) the

comments received are of significant enough importance to delay the release of Data; and/or (b) additional information is required from the requesting party to address the comments -- then the data should not be released until the additional information has been received from the requesting party and an additional review is conducted by the Executive Director or the Data Release Committee, as applicable, to ensure that the Applicant conforms to all applicable requirements of this policy and procedure.

A comment period allowing the public to comment on the proposed data releases and the proposed use of data to be released would strengthen the public's confidence in the data release process utilized by the APCD by providing a clear and transparent process by which individuals would be given an opportunity to address any concerns that may be raised by a data release application.

Limiting Data Uses

We propose that the use of data released by Access Health CT be allowed specifically for research and academic statistical purposes, purposes for the public well-being only and exclude the release of data for commercial purposes that would facilitate collusion or anti-competitive behaviors based on data sources revealed in the data release request. In order to facilitate the purpose of collecting data by the APCD as identified in Connecticut General Statute Section 38a-1091 that includes the purpose of making data available for the purpose of allowing the review of data as it relates to health care utilization, costs or quality of health care services, we believe that the information release should be primarily for research and academic purposes and purposes of the public well-being and should not be release by the APCD for commercial purposes. As detailed above, the data held by the APCD is often considered by Data Submitters to be confidential and propriety in nature, and often a trade secret. The release of the data for commercial purposes to a competitor of a Data Submitter has the potential of causing significant harm not only to the Data Submitter but also to the health care marketplace.

Because a risk of harm detailed above exists when a data release is for a commercial purpose, rather than for research or academic purposes or purposes for the public well-being, we request that the APCD restrict the release of data to research and academic statistical purposes and purposes for the public well-being only and exclude the release of data for commercial purposes that would facilitate collusion or anti-competitive behaviors. If the APCD is unable to restrict all data from being released for commercial purposes, we request that the APCD consider an alternative approach for commercial purposes that would restrict the release of claims and prescription data fields directly related to pricing, payment, and copayment/coinsurance. Potential solutions to address the concerns above include:

- Redefine "*Data Release Application*" in Section 2j. to read: "*Data Release Application*" means the written application and supporting documentation or other materials an Applicant submits to the Executive Director or the Data Release Committee in connection with a request to access Data. The purpose of such application shall only be for research or academic statistical purposes or purposes for the public well-being and no application shall be permitted for a commercial purpose that would facilitate collusion or anti-competitive behaviors.

- Redefine "*Project*" in Section 2t. to read: "*Project*" means the purpose or program for

which Data is disclosed to a Recipient. Such purpose or program shall be for research or academic statistical purposes or purposes for the public well-being only and shall not be for any commercial purpose that would facilitate collusion or anti-competitive behaviors.

- Revise Section 6a. Data Release Application. to read: "The Exchange shall develop and maintain a Data Release Application. The Executive Director shall retain the right, in his or her sole discretion, to modify the Data Release Application for particular Applicants or Projects; provided such modification is consistent with this Policy and applicable law. The proposed use of information requested by any Data Release Application shall only be permitted for research or academic statistical purposes or purposes for the public wellbeing and shall not be permitted for any commercial purpose that would facilitate collusion or anti-competitive behaviors."

Data Release Committee
We appreciate that Access Health CT has committed to including a representative from the health insurance industry to be a part of the Data Release Committee as a committee member. We would encourage Access Health CT to consider a national carrier with experience responding to APCD data release matters when proceeding to select a representative from the health insurance industry to sit on this committee. We believe that a national carrier with experience working across numerous APCDs would bring a beneficial and unique perspective to Access Health CT when reviewing and responding to Data Release Applications.

Thank you, again, for allowing UnitedHealth Group the opportunity to comment on the proposed Access Health CT APCD Privacy Policy and Procedure. Please let me know if you have any questions or concerns regarding these comments.

Sincerely,

Philip N. Anderson
Associate General Counsel and Director
Legal, Compliance and Regulatory Affairs Northeast

Email by Susan Israel, MD - November 24, 2015

Public Comment on the Connecticut All-Payer Claims Database Privacy Policy and Procedure Draft of November 2015. (The concerns below also apply to the intended study of patient electronic health records by the State Innovation Model medical home and by the Health Information Exchange created by PA 15-146.)

First, let us remember that the Connecticut APCD makes health plans submit identified claims data which include health plan enrollment data with family information, patient names, addresses, Social Security numbers, all diagnoses, procedures, tests, drugs prescribed and providers seen, all with dates of service – that is a lifetime medical dossier on each person. This data is then given to "Recipients" (P&P, 2. u., p.3) such as academic researchers and state agencies in forms not safe from re-identification. The danger is that intimate medical information could be used against us in employment, for example, or to pressure a legislator or government official, undermining our democracy. A government agency, the Department of Public Health, already has identified patient data on hospital discharges, newborn DNA, tumors, and sexually transmitted infections, etc. Additionally CT has a controlled substance registry. So this means that a person cannot have a truly private psychiatric admission nor keep the state and many others from knowing that they filled a prescription for an antianxiety medication by a named psychiatrist. And now the APCD will create another data base with all of this information.

In contrast to the citizens of the State of Rhode Island (which does not take names or full addresses), the citizens of Connecticut cannot opt-out of the APCD, even though the Policies and Procedures of the APCD make it clear that the security of patient data cannot be guaranteed against breaches, leaks or re-identification of patient data. (1) Accordingly, Access Health carries cyber-liability insurance to protect itself but then will shift liability to the "Recipients" for any breaches of the data in their possession as they must "… hold the Exchange and the State Harmless from any and all claims, losses, liabilities .... or disclosure of the Data" (P&P, 7.a.i.(xiv), page 12-13).

In many cases, Access Health will not retain electronic control over the data when released to the Recipients (P&P, 7.b.i., page 13), and the "Recipients" can then re-disclose the "Data" to a "Recipient Third Party" (P&P, 2. v., p. 3) which has not been directly vetted by Access Health. Additionally, it is worrisome that Access Health only requires a signature as the proof that the "Data" have been returned or destroyed after use (P&P, 8.c., page 14), given that there is a huge market for medical information. And how would a patient even know if their data was compromised to a wider market?

"Data" is defined as "De-Identified claim information provided to the APCD by Data Submitters and made available through the Vendor or Managed Environment" (P&P, 2.j., page. 2), and "*De-Identified*" refers to healthcare information from which all eighteen (18) identifiers enumerated at 45 C.F.R. § 164.514(b)(2) have been removed (P&P, 2.n., page 2).

However, these definitions do *not* indicate that there will be an exception to the definition of "De-identified claim information" when the "Executive Director may, in his or her discretion, permit

designated APCD Personnel to use a Limited Data Set from the Managed Environment or Vendor" (P&P, 5.b.iv., page 7). This is significant because Limited Data Sets, with only 16 of the 18 identifiers removed (P&P, 2.r., page 3), are more easily re-identified as explained later below.

Also these above definitions do not inform the public that the Vendor, On Point (which will also be doing research with the data), will receive fully *identified* data from the Data Submitters, nor reveal how many Vendor employees will see identified data, how they will be monitored, and how the data will be protected, whether in the cloud or physically guarded in computers on site.

In the case of Gobeille v. Liberty Mutual Insurance which is now before the Supreme Court, Liberty Mutual Insurance is fighting for its right to fulfill its obligation to its health plan customers to protect and control the privacy of their medical data and not turn it over to the State of Vermont's APCD. The main issue is whether or not the self-insured plans that are subject to ERISA must comply with the States' APCD legislation; a secondary issue is patient rights to keep their government from accessing such full medical information without their consent.

In their amicus brief before the Supreme Court, supporting the Vermont APCD in Gobeille v. Liberty Mutual Insurance, the attorneys representing CT's APCD said that the APCD data "fall squarely within the legitimate realm of traditional State policing authority in an area that is firmly within the provenance of the States." So are we comfortable with the State having the right of "policing" powers over our health records and our health care? It could be argued that such "… traditional State Policing authority" was never intended to include such extensive identified medical information about an individual as is required by the CT APCD. Fortunately, the 2nd Circuit Court of Appeals, in its ruling on the Patriot Act, expressed concerns about government's taking of metadata including medical records and whether or not that would be consistent with the 4th Amendment.

The CT APCD attorneys continued in their brief, "… In addition, the APCD will make de-identified[2] health care claims information available to State agencies, insurers, employers, health care providers, consumers of health care services, and researchers "for the purpose of allowing such person or entity to review such data as it relates to health care utilization, costs or quality of health care services." *Id*. § 38a-1091(b)(4)(B).[3]

[2] De-identified health care information is information from which all eighteen identifiers enumerated at 45 C.F.R.§ 164.514(b)(2) have been removed.

[3] For example, oncology researchers may link claims data with tumor registry data (for cancer stage information) and vital… statistics data (for information on death) currently maintained by the State."

In footnote #2 above, the attorneys did not note to the Supreme Court that fully identified data would be handled by a Vendor and that Limited Data Sets, with only 16 of the 18 identifiers removed, would be given to Access Health Employees as stated above. The Limited Data Sets however, greatly increase the likelihood that 63-87% (2, 3) of the data can be re-identified because the Limited Data Sets include the demographics of the full date of birth and full ZIP code (along with the gender). These demographics can then be merged with those of other data bases. The CT voter registration lists, for example, contain the

date of birth, the address, and the *names* of citizens. Also Access Health employees could merge the Limited Data sets with their health insurance enrollment data, which contain patient names, addresses, dates of birth and family information, etc. So realistically, is there a way to monitor or stop an employee from memorizing a set of patient demographics and merging it with other data bases, even on their home computers?

In footnote #3 above, the amicus brief does not note that that Tumor Registry is identified, as are other public health data such as hospital discharge data, etc. (The DPH also hopes to obtain identified outpatient surgical records and possibly health parameters such as smoking and weight as well!) Given that the State of Connecticut's intention is to merge the APCD data with identified Public Health Data and the patient electronic health record from the Health Information Exchange (SB 811, PA 15-146) for study and oversight purposes, how will it be possible to keep the APCD data from being re-identified when it will be mixed so much identified data? The P&P must detail to the public how that technological feat will be accomplished. Even if there might be some masking of the identify of the Public Health data, how will the mixing of so much medical information on a person be accomplished without the identity of the APCD data being revealed? And what will stop the DPH from merging the APCD data with all of the identified data bases that it already has? And the same is true of the handlers of the identified Health Information Exchange data.

Even the fully HIPAA compliant "de-identified" data (18 identifiers removed) that will be given to "Recipients" can be re-identified by several means. D. Lafky of Health and Human Services has shown that HIPAA compliant data with its demographics of *year* of birth, three-digit ZIP for populations greater than 20,000, marital status, ethnicity, and gender have a 0.22% rate (4) of patient re-identification, that is 2,200 people per million or about 7700 people in CT. L. Sweeney showed a .04% rate (5) of re-identification just using year of birth, 3-Digit ZIP code and gender. Both of these rates would be much higher if the accompanying medical histories were merged along with those demographics.

According to the HIPAA privacy rule (which the CT APCD is following even though an APCD is not a HIPAA covered entity), it should be noted that once data is released in HIPAA compliant form, it is no longer subject to the HIPAA Privacy rule even if it can be re-identified subsequently. So if Recipients of the APCD information were able to re-identify it, would they only be subject to a civil suit and fines for breaching their Data Use Agreement as specified in the P&P?

Because of the potential breaches to the health plan claims data, citizens need to have the right to decide for themselves how much risk to their medical privacy they wish to take for the possible benefits to their health care from the APCD program. If the APCD's goal is to increase cost transparency to the medical consumer and even do some quality assessment, it could be accomplished by taking cost and claims data directly from the health insurers without risk to patient privacy. However, it can be argued that the ultimate goal is to use these data to decide which tests and treatments will be offered to patients by the government and insurers. It is debatable that their treatment guidelines/mandates will be accurate and nuanced enough to know what would be optimal medical care for the individual patient, but these guidelines will be the criteria on which the "value" based payments to providers will be calculated. Additionally, the intention is to use cost effectiveness as one of the criteria to define

“value” based care, meaning that not just the medical effectiveness but the cost of the care will now be one of the factors in determining which tests and treatments can be offered to patients without penalizing providers. (6) Patients will lose the full range of choices of testing and treatment options as their providers will be inhibited from suggesting choices that might fall outside of the guidelines, because this will cause financial and professional evaluation consequences to them from any infractions to the guidelines/mandates.

References:

1. Health-Care Industry Spending More on Security But Not Ready for Cyberattack.

Health IT Law & Industry Report: “… FBI Federal investigators also warned Nov. 9 that cybercriminals are increasingly using sophisticated techniques to gain access to health-care organizations’ IT systems. Hackers are “doing their homework” on senior personnel before launching phishing attacks or other campaigns aimed at accessing the troves of personal data health-care companies store, Donald Good, deputy director of the FBI’s Cyber Division, said at the cybersecurity summit. These more targeted attacks can be harder to detect and are resulting in larger and larger breaches of data, he said. ….”

2. Anderson N. “Anonymized” data really isn’t—and here’s why not. Law & Disorder/Civilization & Discontents. Ars Technica; Sep 8, 2009. www.arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/.

3. Sweeney L. Simple demographics often identify people uniquely. Carnegie Melon University Data Privacy Working Paper 3; 2000. http://dataprivacylab.org/projects/identifiability/paper1.pdf. & TheDataMAP. Matching known patients to health records in Washington State data; 2012-2013. www.thedatamap.org/risks.html. & TheDataMap. All the places your data may go; 2012-2013. www.thedatamap.org/.

4. Kwok P. Lafky D. Harder Than You Think: A case Study of Re-identification Risk of HIPAA-Compliant Records. 8. Anderson N. “Anonymized” data really isn’t—and here’s why not. http://www.amstat.org/meetings/jsm/2011/onlineprogram/AbstractDetails.cfm?abstractid=302255.

5. National Committee on Vital and Health Statistics Ad Hoc Work Groups for Secondary Uses of Health Data. Hearing Proceedings; Aug 23, 2007. www.ncvhs.hhs.gov/transcripts-minutes/transcript-of-the-august-2-2007-ad-hoc-workgroup-for-secondary-uses-of-health-data-hearing/.

6. Beck M. Doctors Could be Penalized for Ordering Prostate Tests. The Wall Street Journal.

November 19, 2015.

From: Cappiello, Christine [mailto:Christine.Cappiello@anthem.com]
Sent: Wednesday, November 25, 2015 1:01 PM
To: Salner, Matthew; Lachowicz, Margo
Cc: Cudgma, Anna; sturney@healthcore.com; Hummel, Jill R
Subject: Notice of Intent to Adopt Policies and Procedures regarding APCD

Matt and Margo,

I hope you are well. Below are the comments from Anthem regarding the Notice of Intent to Adopt Policies and Procedures regarding the All Payer Claims Database. They are as follows:

- **Addition:** Include a "Payor representative" to the data request review committee to provide balance on the committee from all pertinent stakeholders, including a representative from the stakeholder that are providing the raw data to the APCD. Rationale - There should be greater participation by the data-supplying entities, who will be able to inform the committee about the potential effects on the data-supplying entities and the market of releasing certain types of data to particular audiences or for particular purposes.
- **Addition:** Institute a process for the purpose of notifying users and providers of health care information when this agency receives a request for health data and accepts that request as a project. Suggestion would be to publish the list of data requests on the Access Health CT website, similar to the manner in which the MHDO publishes requests for data. (See MHDO link for reference.)
- **Definition Change:** section 2.I – "Data" – should include a definition of de-identified claim data. In addition, data available to data requestors should be limited within a data release so that payer specific utilization and payment data cannot be used for anti-competitive purposes. This would require that payer specific utilization and claim data only be made available in aggregate both in published reports and within data sets. For example, in a data set, payer identifiers would not be present if costs and utilization data is provided to a requestor. (Please see the question below on the anti-trust question.)
- **Question** – Will Access Health CT be following the recommendation of the U.S. Department of Justice (DOJ) and the Federal Trade Commission (FTC) (together, the "Agencies"), who have issued guidelines to help distinguish lawful from unlawful information exchanges, surveys, reports, and other data dissemination? See U.S. DOJ & FTC, STATEMENTS OF ANTITRUST ENFORCEMENT POLICY IN HEALTH CARE, Statement 6 (1996) (Statement 6).
- **Addition –** Include a minimum set of vetting rules for data requesting entities. Similar to requirements in NH and ME, there should be some published criteria that a data requesting entity must meet to be qualified to receive APCD data.
- **Addition -** The data release application guidelines should include protections with respect to insurers' provider negotiated rates, which are competitively sensitive. The disclosure of negotiated rates can be used to impair insurers' ability to negotiate effectively with providers, and can promote anticompetitive activity. See accompanying recent FTC analysis.

  https://www.ftc.gov/policy/policy-actions/advocacy-filings/2015/06/ftc-staff-comment-regarding-amendments-minnesota-0

  https://www.ftc.gov/news-events/blogs/competition-matters/2015/07/price-transparency-or-tmi

- **Question – Section 5b.v. –** Would Access Health CT provide a description of the internal APCD data storage and protection rules?
- **Question –** Will access to the APCD data require double authentication? Will the APCD data be encrypted at the record level?
- **Question –** Will data requesting entities be subject to audit?

Thank you and please let me know if you have any questions,

Christine

Christine A. Cappiello

Director, Government Relations Division

Anthem Blue Cross and Blue Shield of Connecticut

(203)677-8318 (o) (860)424-2287 (cell)

Christine.cappiello@anthem.com

Notice of Intent to Adopt Policies and Procedures

In accordance with Section 1-121(a) of the Connecticut General Statutes, notice is hereby given that the Connecticut Health Insurance Exchange (the Exchange) is proposing to adopt the various policies and procedures regarding the All-Payer Claims Database for the purposes of establishing processes for the release of data from the All–Payer Claims Database, and privacy and security protections for the released data, pursuant to Connecticut General Statutes Sections 38a-1091(b)(4) and 38a-1090(2)(B).

Interested persons wishing to present their views on these policies and procedures are invited to do so in writing within thirty (30) days following publication of this notice in the *Connecticut Law Journal* -- no later than November 27, 2015. Comments can be submitted electronically to Margo Lachowicz at margo.lachowicz@ct.gov. (The subject line should read: Public Comment). Comments can also be mailed to Margo Lachowicz, Access Health CT/Connecticut Health Insurance Exchange, 280 Trumbull Street, 15th Floor, Hartford, CT 06103.

The proposed policies and procedures are available at http://www.ct.gov/hix or via email to Margo Lachowicz at margo.lachowicz@ct.gov.

All-Payer Claims Database (APCD) Privacy Policy and Procedure -- Draft

Christine A. Cappiello

Director, Government Relations Division

Anthem Blue Cross and Blue Shield of Connecticut

(203)677-8318 (o) (860)424-2287 (cell)

Christine.cappiello@anthem.com