

MarketScan Data Release and Confidentiality Policies

Last revised on: 1/4/2016

this is an automatic date – it is updated when you save and close the document.

Change Log

Author(s) and Contact Information

| Name | Location | Email | Telephone |
| --- | --- | --- | --- |
| Erica Danielson | Portland, OR | erica.danielson@truvenhealth.com | 503.894.8085 |

Revision History

| Date | Description | Name |
| --- | --- | --- |
| 11-03-09 | Copied text into new outline format. Added new practice clarification that data suppliers shall not be allowed to purchase an extract that excludes certain data. | T. Hubbard |
| 11-5-10 | Updated Section 3B vi. After contractual scrutiny we cannot release any Provider Identifiers (hospital or physician). Aggregated provider results may still be reported. | E. Danielson |
| 7-5-11 | Updated Section 3Aiii to include language specifying that no State or zip code level information for South Carolina may be reported nor can any geographic information be released from the Medicaid database | E. Danielson |
| 2-5-13 | Rebranding with Truven logo | E. Danielson |
| 3-3-14 | Updated Copyright date | E. Danielson |
| 4-9-14 | Update – exclusion of PBM’s for supplier threshold verification section 3.B.xi.c | E. Danielson |
| 1-9-15 | Update the lists of states which cannot report at state level or zip code level. | E. Burleigh |
| 1-4-2016 | Updated the lists of states which cannot be reported at the state level or zip code level | E. Burleigh |

Table of Contents

1. Overview 5

2. Data Contriubution and Use 6

3. Data Aggregation and Release Policies 8

4. Legal Agreements Binding Data Use 10

# Overview

* 1. Protecting the privacy of patient data as well as the privacy of our clients is a core principle of Truven Health Analytics. Without this firm commitment, we risk violation of our contractual agreements with clients and with the HIPAA Privacy Rule. The HIPAA Privacy Rule governs use and disclosure of any Protected Health Information (PHI).
  2. MarketScan is *any* pooled experience of Truven’s Health Plan, Employer, and Government clients who contribute to the MarketScan database. Any internal or external pooling of data from more than one Payer client is considered to be a MarketScan product or analysis. When permission is given by a client to contribute their information to MarketScan, the data may be included in one of four types of products:
     1. Patient-level data files which have been statistically de-idntified and are no longer in need of the protection of the HIPAA Privacy Rule
     2. Analyses, norms, or other summary products developed from the de-identified patient-level data files
     3. Studies that pool data from clients to produce information that relates to the health care operations of the clients (HIPAA refers to these studies as data aggregation studies)
     4. Research projects which pool a limited data set version of data from clients
  3. Other pooling of data is not allowed under the HIPAA Privacy Rule. For example, you may not pool data that has not been de-identified and provide it to a single Truven client.
  4. Truven is contractually obligated to protect the privacy of our clients and the employees, retirees, and dependents covered by their plans. This protection is outlined in either the Services Agreement and/or the Data Contribution and Use Agreement coupled with the HIPAA Business Associate Agreement. The MarketScan Data Confidentiality and Data Release policies address our principles, legal requirements and our current practices regarding patient, client, and data supplier confidential data, data masking and encryption, and release to third parties.
  5. **The policies described in this document must be utilized by Truven staff whenever data are pooled for an external purpose.**

# Data Contriubution and Use

1. Definition of Terms:
   1. Data Contributor – A data contributor, or “client”, has signed an agreement with Truven to contribute their data for inclusion in the MarketScan databases and data aggregation products.
   2. Data Supplier – A data supplier, or “carrier”, submits data to Truven on behalf of the data contributor (i.e. health plan submits data on behalf of employer).
2. Overview:

Data can be pooled only if there is a legal agreement granting Truven rights to use a specific client’s information. The details of this agreement may be outlined in the Services Agreement or in the Data Contribution and Use Agreement (DCUA) as a separate exhibit. The agreement exists between the Client and Truven and allows Truven to use the data for its business purposes, including the right to de-identify and license the data for inclusion in MarketScan databases and data aggregation products. This agreement also sets forth strict requirements to protect the data with respect to client confidential information and patient privacy/confidentiality.

1. Data Contribution Levels:

Two types of data contribution levels are described below. The MarketScan data release policies outlined in this document must be followed regardless of whether a client is a “full” or “partial” data contributor.

1. Full Data Contributor - A full data contributor is a Truven client who has signed the Data Contribution and Use Agreement without substantial modification.

The following are the data contribution requirements:

* 1. Client agrees to include Truven minimum data elements in client databases. The variable list is available to Truven sales staff and may be included in the client's services agreement (Exhibit A).
  2. Client allows Truven to retain the client’s de-identified data in MarketScan databases, norms, and other MarketScan products which can be used, licensed, and disclosed subject to the confidentiality provisions included in the agreement.
  3. Client provides the data free of encumbrances or restrictions.

1. Partial Data Contributor - Many of our clients rely on data suppliers to provide needed information for our decision support systems. If a client’s data supplier refuses to release certain information for contribution to MarketScan, it may compromise the client’s status as a full data contributor (i.e., the client may no longer be a recipient of MarketScan norms free of charge). To be considered a *full* data contributor, the client must provide *all* data elements necessary to build MarketScan norms, research databases, and other products.
2. Exceptions
   1. Any exceptions to the data contribution policy require the approval of the General Manager responsible for the market sector of the data contributor involved.

# Data Aggregation and Release Policies

1. Principles - The following are the principles for use of the data used in MarketScan products and analyses and must be followed by all employees when creating a data extract for a client deliverable or performing any study which aggregates data from more than one client:
   * 1. No data may be used without the permission of the client (as noted in DCUA or Services Agreement).
     2. MarketScan patient-level files are de-identified according to HIPAA standards.
        1. Explicit individually identifiable data elements (e.g. enrollee names, street address, social security numbers, health plan beneficiary numbers) received from our clients are not retained.
        2. The MarketScan patient-level files use synthetic enrollee/patient identifiers based on a combination of variables. These variables include the gender, relationship to the contract holder, client, and the health plan beneficiary number. This combination of variables makes it impossible to link the synthetic identifier back to a scrambled social security number.
        3. Only the following variables are released: synthetic patient identifier, age, year of birth, and 3-digit ZIP.
     3. No MarketScan data, norm or research study will be released that discloses the identity of a client without the written permission of the client.
        1. No norms, benchmarks or extracts can be released at the state or zip code level from our CCAE for **Connecticut, Maine, New Hampshire, Indiana, South Carolina, West Virginia, Louisiana, Idaho, New Mexico, and California.**
        2. No norms, benchmarks or extracts can be released at the state or zip code level from our Medicare Supplemental data for **Connecticut, Maine, Massachusetts, New Hampshire, Michigan, Delaware, South Carolina, Louisiana, Colorado, Idaho, New Mexico, and California.**
        3. **No geographic identifiers** may released when analyzing the **Medicaid** database
   1. Practices - The following are our current practices:
2. Norms or research studies based upon a specific data supplier may not be released.
3. With the exception of the Multi-State Medicaid Database, a data contributor can purchase an extract of only their data or an extract that excludes their data.
4. A data contributor (or customer who may not be a contributor) cannot purchase an extract that excludes certain data contributor(s) or data supplier(s) other than themselves.
5. Data suppliers (who are not also data contributors) shall not be allowed to purchase an extract that excludes certain data contributors or data suppliers.
6. Hospital identifiers supplied by a client are encrypted in any licensable database released externally. If the client's and/or the data supplier's agreement has specifically prohibited the release of hospital identifiers, those restricted identifiers will be blanked out/set to missing before releasing the licensed database.
7. For custom projects, unencrypted provider identifiers may be used to aggregate specific hospitals or physicians and report on the aggregated results as long as Section 3B xi release guidelines are still met.
8. For internal studies, any unencrypted hospital identifiers may be used (both restricted and non-restricted). However, we cannot release any outcomes, benchmarks, etc containing the restricted hospital identifiers.
9. Confidential negotiated payment arrangements between payers and providers cannot be released*.* Provider-specific discount information supplied by a client may be released only to that client. Data extracts can include submitted charges or allowed amounts, but not both. When purchasing a data extract, a customer can choose one of the two financial measures; however the customer will be “locked in” to that selection for any future data purchases. Norms of discounts (not provider-specific) which follow the three standard data aggregation rules below can be produced.
10. For custom projects, customers can purchase allowed amounts or submitted charges (not both) for a requested list of hospitals as long as 1) the three standard data aggregation rules are met and 2) the contributors/data suppliers did not contractually prohibit the release of the requested hospital identifiers.
11. Normative data or benchmarks must be based on a denominator size of at least 30 admissions, patients, records, etc. Norms with a denominator size less than 30 must be approved by the Practice Leader or General Manager of the operating unit.
12. The following three requirements are also current practices when creating a norm/benchmark or data extract. However, it is possible that on occasion, the information desired may not be able to be gathered using all three. The Practice Leader or General Manager of the Operating Unit may approve an exception to these rules:
    * 1. **A data extract or benchmark must be composed of at least 3 data contributors.**
      2. **No single data contributor may make up more than 60% of the population or 60% of the denominator for the benchmark (e.g., admissions).**
      3. **No single data supplier may make up more than 70% of the denominator for the benchmark (e.g., admissions). In cases where the denominator represents membership which is not stratified by supplier, then no single data supplier may make up more than 70% of the patients included in the numerator. Note, Pharmacy Benefit Manager’s (PBM) are excluded from supplier verification.**

# Legal Agreements Binding Data Use

1. In order for data to be used in MarketScan, other legal agreements may bind our use of client data. These agreements also protect the confidentiality of the clients and data suppliers.
2. In addition to the Services Agreement and/or DCUA, the following agreements stipulate use of client data:
   1. Hold Harmless Agreement/Confidentiality Agreement

The Hold Harmless Agreement is a legal document. The Hold Harmless Agreement restricts the use of data or disclosure to third parties and indemnifies the data supplier from any breach of confidentiality of the data released by the data supplier. This means that Truven is fully liable for any breach of confidentiality by Truven. The agreement may also describe how the data will be encrypted and protected. This agreement may be required by a data supplier and is a three-way agreement between Truven, the client, and the data supplier.

* 1. Business Associate Agreement

The Business Associate Agreement is a separate agreement between the client and Truven. The HIPAA privacy rule dictates that any party who receives protected health information to use on behalf of a covered entity or a plan sponsor, as defined under HIPAA, must sign a Business Associate Agreement with the covered entity or plan sponsor. The agreement must contractually bind the party to abide by the HIPAA privacy rule in the same manner that would be required by the covered entity or plan sponsor.

The agreement contains the following conditions which relate to MarketScan:

* 1. Truven may use the data to perform data aggregation services for the client.
  2. Truven may de-identify the data and use the de-identified data in commercial applications
  3. Upon termination of the product and services agreement between the client and Truven, Truven will destroy all copies of the original protected health information or return them to the client or data supplier.

1. Data Use License Agreement (DULA)
   1. The Data Use License Agreement (DULA) is a legal document describing the terms and conditions under which the client may use or license the MarketScan data.
   2. The DULA contractually prohibits external data linkages between MarketScan data and other private or public data sets for the purpose of identification of employees, beneficiaries, patients or other individuals.
   3. If the identity of any person or establishment is discovered, the DULA prohibits use of this information.
   4. The DULA further prohibits unauthorized transfer of the data.