Reporting to Payers, Regulators, and Managers: Some issues and Experiences with Confidentiality and Compliance

Richard R. Carlson
Medica
401 Carlson Parkway
Minnetonka, MN 55305-5387
rick.carlson@medica.com

Abstract

When dealing with Protected Health Information (PHI), care must be used to maintain confidentiality. At the same time, demands are made for reporting activity and at levels that may cause risk for confidentiality. This paper describes some of the experiences and methods used to maintain confidentiality and proposes a solution to the problematic reporting of small populations.

Keywords: Confidentiality, HIPPA, Compliance

1. Introduction

Medica is a regional health plan / health insurance company that serves Minnesota, and parts of Wisconsin, North Dakota and South Dakota. The plan covers about 1.2 million people under a variety of products including fully-insured, self-insured and market segments (commercial, Medicaid, and Medicare). Medical holds Excellent Accreditation from NCQA for commercial as well as Medicaid products and was named one of the Top 25 Medicaid Plans by USNews and World Report.

The plan reports a variety of utilization measures – hospitalizations, ER visits, outpatient visits, and drug usage.
For most large populations, these rates can provide useful indicators of cost or appropriateness of care. However, this can cause problems with many populations as the incidents of utilization may be small.

This paper's genesis began with the problem of determining what can be reported to employers about their population's experience with Disease Management. Health Care Data (claims, utilization, and medical records) is governed by HIPAA

2. HIPAA

HIPAA is the Health Insurance Portability and Accountability Act. It defines protected health Information (PHI) as health information that is individually identifiable (e.g., member-specific) and that is created, maintained, used or disclosed by or for Medica. More specifically, the term refers to information that:
(i) identifies or could reasonably be used to identify the individual; and
(ii) relates to:

> (a) an individual's physical or mental health or condition;
> (b) the provision of health care to an individual, or
> (c) payment for health care provided to an individual.

The goal is to report these utilization rates without inadvertently providing identifiable information as there are both civic and criminal penalties. Under US Code 42USC1320d-5 the general penalty for failure to comply with requirements and standards is:
(a) General penalty
(1) In general
Except as provided in subsection (b), the Secretary shall impose on any person who violates a provision of this part a penalty of not more than $100 for each such violation, except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed $25,000.
It also defines the wrongful disclosure of information as: 42USC1320d-6 Wrongful disclosure of individually identifiable health information
(a) Offense
A person who knowingly and in violation of this part-

> (1) uses or causes to be used a unique health identifier;
> (2) obtains individually identifiable health information relating to an individual; or
> (3) discloses individually identifiable health information to another person, shall be punished as provided in subsection (b).

(b) Penalties

A person described in subsection (a) shall-

(1) be fined not more than $50,000, imprisoned not more than 1 year, or both;

(2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and

(3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.

While there have been very few prosecutions for violations of HIPAA, it still functions as a deterrent as few organizations wish to find themselves in a media headline for violating health care privacy.

Specifically, PHI information is member information that includes any of the following elements:

- Names, Telephone numbers
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geo-codes, except for the initial three digits of a zip code
- E-Mail Addresses, Social Security Numbers
- Medical Records Numbers, Health Plan Beneficiary Numbers Account Numbers Certificate/License Numbers
- Vehicle Identifiers and Serial Numbers (Including License Plate Numbers)
- Biometric identifiers, including finder and voice prints
- Device identifiers and serial numbers Web URL's IP Address numbers
- Any other unique identifying number, characteristic, or code (excluding a code or record identification number that would allow the covered entity to re-identify the information but that is not related to information about the individual or capable of being translated to allow identification of the individual).

While the above is an expansive set of data that needs safeguards, HIPAA also provides rules of use. Those rules include: "… may use and disclose protected health information for purposes of payment, treatment and health care operations ("TPO") without a signed authorization as follows:

(i) for its own payment or health care operations activities;

(ii) for treatment activities of a health care provider;

(iii) to a health care provider, health plan or health care clearinghouse for that entity's payment activities; or

(iv) to another entity covered by HIPAA for that entity's health care operations, if that entity has a relationship with the individual, the information relates to that relationship, and the disclosure is either for fraud and abuse detection or compliance, or for one of the purposes listed in paragraphs (i) or (ii) of the definition of health care operations".

HIPAA also provides for Exceptions. Written authorization must be obtained for the following TPO uses and disclosures of protected health information:

(i) disclosure of the individual's clinical medical record or chart, except as permitted under applicable state law;

(ii) disclosure of substance abuse treatment program records, except as expressly permitted under 42 Code of Federal Regulations Chapter 1;

(iii) use and disclosure of psychotherapy notes, except as expressly permitted under HIPAA; and

(iv) any other TPO disclosure which requires written authorization.

3. De-Identification

One way to protect PHI is to de-identify the data – that is strip the data of fields that can be used to identify an individual. These include:

- Names
- All geographic subdivisions smaller than a state, … except for the initial three digits of a zip code
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death;
- Telephone numbers
- Fax numbers
- E-mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers

This strategy works as long as the counts or volumes are enough to hide individuals. In small groups the hospitalization, ER visit, or number of people with a diagnosis may identify an individual.

4. Central Conflict Regarding Data

The central conflict regarding data is that payers want to see what happens. They want to know what they are paying for. This is especially important as the cost of health care (and insurance) has risen. However, to see what happens, they often want to hear the story of care – which is PHI.

One way to tell the purchaser what happened is to share frequencies and utilization rates for the population for which they are paying. But, for rare events, the very identification of an event may be enough to identify an individual; thus violating HIPAA. So the big question becomes "How Small can you go?"

For small populations, the incidents of some utilization measures (Admits, ER visits, Rx use, etc.) are infrequent. Those events when combined with a small population may allow for individuals to be identified.

Examples: For a small employer, everybody may know that Jane or John was in the hospital last month or that Jane or John's child was in the ER room during that period of time. But if we report that rate, cost, or diagnosis, then that release of information may be a violation of HIPAA.

5. Self-Insured are Different

Insurance companies (including HMOs) generally have sufficient populations to report rates while still protecting PHI. They do not have to report to individual employers (insurance purchasers) on their populations. However, self-insured are different. Since they are taking the financial risk, they generally want to see what they purchased to manage their costs. So, the self-insured employers can legally see everything they need for TPO. Some organizations want to see everything. Others are wary of HIPAA and want no part of anything that remotely approaches PHI.

6. What to Do

There are a number of options for reporting to self-insured.

The null position is to report nothing. This is not really feasible as you will not retain customers telling them nothing.

Option 1: The first option is to report in plan aggregate only. This option is to report only the plan data to the employers. They would receive no data specific to their employees. This is the next least desirable alternative for the employers.

Option 2: The second option is to reports subsets of aggregate only. An example of this is to report diabetes statistics for the plan, but not diabetes statistics for the employer's population.

Option 3: The third option is to report employer data if their population is large enough to sufficiently hide individual detail.

The last option (for self-insured only) is to allow employers to see detail with the requirement of signing a waiver that they are using the data for health care operations.

6.1 Operational Issues

The above options have a series of questions and concerns to make them practical.

6.1.1 Thresholds

The first question is how much is enough. What are the thresholds for enough data? Some organizations use three as the minimum cell size of reportable data. This means 3 hospital admits, 3 people with a diagnoses, etc.

6.1.2 Minimize cross tabular tables

This may be the biggest threat to PHI. Crosstabs can reduce cell sizes very quickly. If the tables can be linked with other tables or rates, then the potential for identification increases.

6.1.3 Degrees of Freedom

Suppression of cells because they contain small values is an important technique. Suppressions may require either not reporting cells or combining cells, rows or columns. However when suppressing cells, one must make sure that the suppressed cells cannot be inferred. The simplest way is to make sure that the suppressed information cannot be solved for. This becomes more complex with large tables and linked tables.

6.1.4 Simplicity

Simplicity is an important characteristic of any operational rule. As Einstein stated, "Things should be

made as simple as possible, but not any simpler." Simplicity also allows for easy programming. Complexity will encourage short-cuts which will violate the rules and lead to unintended disclosure.

6.1.5 History Rules

Data and reporting are part of a continuum. People will remember what was reported in the past and may (probably will) compare it with the current report. It totals such as Year-to-date are reported then they may be able do discern suppressed data.

6.2 Example of Small Population Reporting

The impetuses for this paper were problems with Disease Management reporting. Disease Management manages people with specific conditions (such as Diabetes, Coronary Artery Disease, Multiple Sclerosis, etc.). Each condition typically covers less than 5% of a general healthy population. About 72 out of 1000 people in our commercial population have the conditions covered in disease management. Half of those are diabetics and 20 in 1000 are pediatric asthmatics. The rest cover a variety of diseases.

Suppose that an employer has 1000 covered lives, then about 70 people are covered by Disease Management, with about 35 diabetic and 20 are pediatric asthma. Heart Failure has about two (**2**) people! So any statistics on Heart Failure (including the fact that there are two becomes problematic). And this is for a group size of 1000!

6.3 A Potential Solution

We created summary reports that use options 1 (plan aggregate), 2 (disease or product aggregate) and 3 (employer data with enough population). The plan aggregate is reportable for those conditions where so rare that almost any subset of our overall population would potentially disclose PHI. Generally, we will report disease aggregate for our population or for an entire product (such as commercial, Medicaid, or Medicare). For those employers with large enough populations and rates of occurrences we will report their rates. For self insured payers with appropriate signatures and waivers we will also provide detail.

7. Future

For those groups with small populations, they still want to know what is happening and one idea that we are considering is to report expected values and confidence intervals around those expected values. This assumes that the population at risk is reportable (e.g. greater than 3). This option give the employer the likely number of occurrences and the expected range (we can use 80%, 90% or 95% intervals), but it will not give the actual number of occurrences. Since the range of likely values is displayed, this helps show the potential problems with reporting small values. For example, given an overall occurrence rate of 200 per 1000 members per year and you have 60 covered lives, the number of occurrences in a quarter (three [3] months) is three (3) with expected bounds of zero (0) and seven (7). Similar calculations can be made for monthly or half-yearly reporting.

8 Speculation

This method of reporting expected values with confidence limits has potential applications for other small group reporting, not just for disease management. Routinely, small groups want to see their various general utilization rates for their entire population (not just the disease management population), but the expected variation is quite large and may border on exposing PHI. This strategy reduces exposure of reporting identifiable data and still provides the general approximation of what they are likely to experience.