The Sleeping Dragon Stirs:
The Dawning of Section 1104 Regulatory Enforcement

Matthew Albright
Zelis Healthcare
December 2016

zelis™

Though silent in terms of new regulations, CMS has turned its attention toward developing its enforcement capabilities to focus on the HIPAA transaction regulations it has published. Health plans and their business associates are likely targets.

In 2011, the Centers for Medicare & Medicaid Services (CMS) began spitting out regulations at the rate of one every 6 months in order to propagate Section 1104 of the Affordable Care Act (ACA) on behalf of the Department of Health and Human Services (HHS). Section 1104 was designed to bolster the mandates of HIPAA administrative simplification that had been passed by Congress 15 years before. ACA's new additions to HIPAA administrative simplification promised to re-invigorate the push to move the healthcare industry toward conducting the transactions electronically and taking a bite out of the estimated $40 billion in wasted money and resources in U.S. healthcare administration.

In quick succession, operating rules on eligibility, claims status, EFT healthcare payments, and electronic remittance advice transactions were mandated. A Health Plan Identifier (HPID) was adopted through a final rule, and an HHS Certification of Compliance program was proposed. The penalties described for the HHS Certification of Compliance program came directly from the ACA and they were hefty: One dollar per covered life of the health plan per day for every day that a health plan didn't meet the requirements of the program.

"There continues to be a perception that there are no consequences to not being in compliance with the adopted standards and operating rules, so my group is developing a comprehensive compliance strategy that will challenge that perception."

– Shana Olshan, Director of the National Standards Group (NSG), Centers for Medicare & Medicaid Services. *February, 2016*

As was true with the original HIPAA administrative simplification requirements mandated through regulations in the early 2000's, the burden of meeting these requirements falls almost wholly on insurers, group health plans, and other payers that met the definition of HIPAA-covered health plans and their business associates, such as TPAs. Providers have very little in the way of requirements, and have virtually no worries in terms of enforcement or fines.

But after January 2014, there was silence. No further Section 1104 regulations have been released in the nearly three years since publication. The group responsible for the regulations, CMS' National Standards Group (NSG), seems to have gone dormant, leaving many of the Section 1104 mandates without enforceable regulations and, in some cases, reversed. In 2015, for example, enforcement of the HPID final rule was postponed and the proposed rule for the HHS Certification of Compliance program was pulled to be re-drafted.

Don't Mistake Silence for Safety: Audits are Coming

A seeming lack of inactivity may be leaving health plans and their business associates with a false sense of security about compliance, as it appears that the regulations that survived had no teeth. But underneath the surface, NSG has not been idle: It's been focusing on its enforcement capabilities.

The biggest indicator of this comes from the group's change in leadership and reorganization in 2014. NSG went from having only one FTE employee with enforcement duties to establishing a whole division on enforcement named, predictively, the Division of Administrative Simplification Compliance.

Very quickly, this new division made it clear that it was concentrating on developing a "comprehensive compliance strategy" that included two separate approaches to enforcement:

- **Enhancing NSG's infrastructure for fielding complaints alleging non-compliance**
  Part of NSG's enforcement focus after 2014 was to give a face-lift to its reactive, complaint-based process for investigating alleged violations and to actively solicit complaints of possible non-compliance. This past summer, NSG unveiled a new and improved version of its Administrative Simplification Enforcement and Testing Tool (ASETT), an online application where individuals or organizations can submit complaints of non-compliance with the option to file anonymously.

  At the same time, NSG began a vigorous marketing campaign for ASETT directed at providers and trading partners, urging them to use the tool to file complaints against organizations that are not complying with the standards and operating rules.

  As the industry becomes more aware of ASETT, complaints of non-compliance against organizations appear to be growing. NSG has stated that an average of 500 complaints a year have been received in the past few years through the system.

ASETT

CMS recently unveiled a new and improved version of its Administrative Simplification Enforcement and Testing Tool (ASETT), an online application where individuals or organizations can submit complaints of non-compliance. NSG is marketing this tool to increase awareness.
https://htct.hhs.gov/asett/public/home.act

ASETT and the ASETT website are property of the Centers for Medicare & Medicaid Services

- **Establishing an audit program as required by ACA Section 1104**
  NSG has also publicly stated that it is working on the audit program that the ACA requires it to develop. As a hint of things to come, the National Committee on Vital and Health Statistics (NCVHS), the Federal Advisory Committee that is responsible for making recommendations to HHS on the HIPAA transactions, has recommended that the audit program be modeled on the much-hyped audit program set up by the HHS Office of Civil Rights (OCR) on HIPAA privacy and security.

In addition to these developments, the director of NSG, Shana Olshan, recently promised that an enforcement strategy for HIPAA transaction requirements was on its way.

Reading the Signs: What will Section 1104 Enforcement Look Like?

Because NSG shares the same regulatory powers and enforcement tools as OCR for HIPAA privacy and security, a good guess would be that NSG's enforcement strategy will be similar to the strategy being employed by OCR.

NSG and OCR have a lot in common:

- The requirements around both the HIPAA transaction sets and the privacy and security standards ***share the same section*** on enforcement in the Code of Federal Regulations (45 CFR §160), and most of the enforcement processes and penalties are the same.
- Although the requirements for privacy and security are vastly different from the HIPAA transaction standards, both NSG and OCR have authority to use the same enforcement tools:
  - Both use the reactive complaint system as a way to line up candidate organizations for investigation
  - Both NSG and OCR can conduct compliance reviews to investigate allegations of violations of HIPAA Rules brought to their attention through mechanisms other than a complaint (78 CFR 5579)
  - Both can use audits as a tool, and both can levy the same maximum civil money penalties per violation
- Most importantly, both have no limit to the amount of civil money penalties that they can assess to any given entity if there are multiple provisions that have been violated or if the violations affect many different people

One difference between OCR's audits and NSG's promised audits is that NSG may skip over the multi-year piloting of the program that OCR went through. The Health Information Technology for Economy and Clinical Health Act (HITECH), passed in 2009 required the OCR audits; OCR conducted the audit pilot program in 2011, and then started Phase I audits in 2012. The testing of a HIPAA audit program has already been done, so NSG may opt to forgo it and get right to business.

> *"HHS should... consider enforcing compliance with the adopted standards and operating rules with the same level of engagement seen in the OCR HIPAA Privacy and Security Compliance Program".*

– National Committee on Vital and Health Statistics (NCVHS), the Federal Advisory Committee that is responsible for making recommendations to HHS on the HIPAA transactions, *October, 2016*

Using a Not-so-Secret Weapon, Non-Compliance May Be Costly

Using these similarities as sign posts, we can begin to map out a picture of what future Section 1104 enforcement may look like.

OCR has exercised all of the enforcement approaches allowed to it by law. Of note is one particular, rather stealth weapon of enforcement that OCR has used with a certain artfulness, and NSG may employ with the same finesse: ***resolution agreements.*** Resolution agreements for the HIPAA-violator are a kind of plea bargain to avoid much larger civil money penalties. This strategy results in violators paying fines one way or another.

The resolution agreement is employed like this: When an organization's violations are discovered – either through a complaint investigation or compliance review – OCR calculates the possible civil money penalties which, again, have a maximum limit per violation but have no maximum limit overall when multiple violations are found. And there are always multiple violations.

On top of this, the OCR's civil money penalty (CMP) calculations are purely subjective; in fact, regulations actually require that OCR calculate CMPs on a case-to-case basis using 14 different "mitigating and aggravating factors," including the violator's financial status, past compliance history, and the all-encompassing "other matters as justice may require"(45 CFR 160.408).

> *"These settlement agreements have involved the payment of a monetary amount that is some fraction of the possible CMPs for which the covered entity or business associate is liable in the case."*
>
> – Office of Civil Rights in a report to Congress. *2015.*

Facing very high CMPs, organizations agree to resolution agreements in which they are allowed to pay an ***agreed-upon lesser amount*** in lieu of the CMPs. In fact, OCR has made headlines not on its CMPs, but on the settlements it has made through resolution agreements – ***$46 million worth since 2011.*** Looking at the public list of HIPAA violations, OCR has only assessed CMPs in two out of 41 cases for a total of $4.5 million. All the rest are "plea bargains" through resolution agreements.

Developing a Playbook for the Future

While NSG has yet to launch its audit program, health plans should use this downtime in HIPAA transaction regulations coming out of CMS as a crack from a starting pistol to do all they can to make sure their systems are "complaint-proof," "compliance review-proof," and ready for the expected audits. This is especially true if a health plan hasn't looked closely at some of the HIPAA transaction requirements.

Assessment

Health Plans and business associates alike should make sure that they are using the most basic HIPAA transactions. HHS is clear that health plans, or the business associates working on their behalf, must have the ability to send the basic HIPAA transactions electronically. The following transactions are likely to be focused on since they all have both adopted standards and adopted operating rules (outlined in table 1) and nearly all payers conduct these transactions either electronically or via paper/paper check/portal/phone.

- **Eligibility Request Response:** the ability to respond electronically to electronic eligibility requests.
- **Claim Status Request Response:** the ability to respond electronically to electronic claim status requests.

- **Health Claim Payments via EFT:** the ability to send compliant claim payments via the ACH network. NOTE: Offering only virtual cards does not fulfill any HIPAA transaction requirements; payment via the ACH network must be offered. A compliant Healthcare EFT includes:
  - The NACHA standard CCD+ Addenda with CORE-required Minimum Data Elements must be sent for the ACH payment initiation
  - The ACH payment and its associated X12 835 must be sent within three days of each other
  - To enroll providers to receive payments via EFT, rules around the data that can be collected must be followed
- Electronic Remittance Advice (ERA): the ability to send electronic remittance advice associated with an EFT. A compliant Electronic Remittance Advice includes:
  - The X12 standard 835 must be used
  - To enroll providers to receive the X12 835, rules around the data that can be collected must be followed
  - Uniform sets of claim adjustment/denial codes (CARC/RARC/CAGC) must be used
  - The ACH payment and its associated X12 835 must be sent within three days of each other
  - Requirements on security and connectivity must be followed

Table 1: Transactions with Adopted Standards and Operating Rules

Transaction	Mandated Standard(s)	Mandated Adopted Operating
Eligibility for Health Plan	• ASC X12 270/271 TR3: Health Care Eligibility Benefit Inquiry and Response April 2008, ASC X12N/005010X279	• Phase I and Phase II CAQH CORE Operating Rules, March 2011
Health Care Claim Status	• ASCX12 276/277 TR3: Health Care Claim Status Request and Response August 2006, ASC X12N/005010/X212 (plus Errata)	• Phase II CAQH CORE Operating Rules 250: Claim Status Rule • Phase II CAQH CORE Operating Rules 270: Connectivity Rule
Health Care Electronic Funds Transfers (EFT)	• NACHA Corporate Credit or Debit Entry (CCD) with Addenda Record (CCD+ Addenda) • For the CCD Addenda Record ("7"), Field 3: TRN re-association Trace Number from ASC X12 835	• Phase III CAQH CORE EFT & ERA Operating Rules, June 2012 includes: - Minimum Data Elements in CCD+ - CCD+ and X12 835 released within 3 days of each other - Enrollment data collection rules for EFT and X12 835 - Uniform sets of claim adjustment/denial codes - Requirements on security and connectivity
[Electronic] Remittance Advice (ERA)	• ASC X12 835 TR3: Health Care Claim Payment/Advice April 2006, ASC X12N/005010X221	

Beyond Implementing the Standards and Operating rules, how can TPAs be Ready for Future Compliance Reviews or Audits?

- While the Certification of Compliance program has not been mandated through regulation yet, TPAs and other business associates may do well to get certified without a mandate. Getting ahead of the curve on this program will act as a "belt and suspenders" to protect TPAs.
- Make sure all your vendor/business associate contracts include a requirement of compliance with HIPAA transaction standards and operating rules. Require CAQH CORE Certification, accreditation by Electronic Healthcare Network Accreditation Commission, and/or other certificates/accreditations or evidence of third party testing. Documentation of third party testing will help deflect any suggestion of "willful neglect" of meeting requirements.
- Remember that certifications and accreditations are a "snap shot" of the ability of an entity to conform with rules and standards at a particular time and can never test for all possible permutations of compliance. A certification or accreditation does not mean that your vendor/business associate is using standards and operating rules on a daily basis to improve your revenue cycle. Ask your vendors/business associates how

they are using compliant electronic transactions to give you better cash flow, greater accuracy, and reduced expenses.

- To prevent complaints, make sure you and your vendors' help desks are knowledgeable about HIPAA transactions.

Evaluating Payment Partners

If the resources required to meet compliance are cost or resource-prohibitive, contracting out services is the most efficient answer.

To cover EFT/ERA standards, payment partners can not only offer compliance, but also reduce a payer's costs by actively enrolling providers into electronic payment programs, which reduces print and postage overhead costs. However, in order for payers to truly realize cost and time savings, healthcare Providers must accept the payments. When evaluating a payment partner, there are several factors to consider beyond valid CAQH CORE Certification. It is important to ask the following questions:

- **Does your payment partner offer compliant options to all providers?** HIPAA mandates that health plans or their business associates must provide EFT through the ACH and ERA to any and all providers only when they request them. This caveat in the regulations leaves room for payment partners to employ efficiency algorithms, which pre-select the providers who will be offered EFT options and who will receive other methods of payment. In fact, some will automatically send virtual cards to providers with no prior notification. This leaves the onus on the healthcare provider to ask for EFT delivery instead. This practice leads to provider dissatisfaction and, furthermore, may lead to provider complaints. A payment partner that offers providers a choice during enrollment prevents any misunderstandings or frustration.
- **Is your payment partner enrollment opt-in or opt-out?** The algorithm method as described above is one where the provider is automatically enrolled, which again leaves the onus on the provider to take action of opting out. Opt-out models such as this not only cause frustration, but they erode provider trust and result in an increased amount of provider noise. Allowing the provider to choose their payment results in much less noise from providers, because an opt-in model ensures that the provider has a) agreed to take the payment electronically and b) is receiving the electronic payment via their preferred method.

- **What additional value does the payment partner offer?**
  It's not enough for a payment partner to deliver compliant payments and data. In order to encourage adoption among providers, payers must evaluate the services a potential partner can offer and the value it can bring to the payer and providers. Does the payment partner offer solutions which solve provider problems? Does their solution offer operational efficiencies? Do they stand behind their products? What does their service model look like?

"We had concerns about how providers would feel about receiving electronic payments and the service levels that they would receive. Those concerns were quickly overcome by Zelis Payments, because it (adoption of e-payments) has started easily and has grown quickly."

– President, Zelis Client

- **How do they ensure the quality of their data?**
  The ability to make accurate payments and move large amounts of data for hundreds of payers is a crucial requirement, but the quality of the data should also be taken into account. Consider a payment partner who has built integrations into the claim payment platforms of their payers. This allows the payment partner to capture data beyond "check level" data, extract the adjustment codes, and create 100% clean and balanced 835s. Clean and balanced data offers value throughout the payment chain as it allows providers to easily reconcile and more accurately bill, which ultimately improves your value proposition.

Conclusion

With regard to ACA Section 1104, HHS has appeared to have been slumbering for the last couple of years, but, as this paper points out, there are several indicators that it's been building up its enforcement strategy and infrastructure and is on the verge of awakening. If OCR's enforcement program serves as a model for Administrative Simplification enforcement, insurers, group health plans, TPAs and other payers will be at risk, and should take this time to assess their current state of compliance and put together any plans to close any gaps they might find. Certainly, third-party partners represent a solution to time- and resourced-strapped organizations, but careful investigation may be required to ensure that these vendors deliver both compliance and employ practices that also deliver value.

Matthew Albright is VP of Legislative Affairs at Zelis Healthcare. Albright previously headed up the Certification program at CAQH CORE and served in multiple roles at the Office of E-health Standards and Services in the Centers for Medicare & Medicaid Services (CMS).