Establishing a Tamper-Resistant Prescription Program

A consultation on how prescription issuers can deter fraud and address legislation mandating use of tamper-resistant prescription pads.

In May of 2007, Congress passed legislation[1] requiring the use of tamper-resistant prescription pads under the Medicaid program. In August, the Director of the Centers for Medicare and Medicaid Services (CMS) issued a letter[2] to all state Medicaid Directors offering guidance on the definition of "tamper-resistance" and implementation of this law.

CONTENTS

THE LAW

In its letter, CMS provided the following instruction:

"To be considered tamper resistant on October 1, 2007, (The deadline was later extended by Congress to April 1, 2008) a prescription pad must contain at least ONE of the following three characteristics:

- One or more industry-recognized features designed to prevent unauthorized copying of a completed or blank prescription form;
- One or more industry-recognized features designed to prevent the erasure or modification of information written on the prescription by the prescriber;
- One or more industry-recognized features designed to prevent the use of counterfeit prescription forms.

No later than October 1, 2008, to be considered tamper resistant, a prescription pad must contain **ALL** of the foregoing three characteristics."

This paper is intended to serve as a guide for assisting issuers in proactively adapting their written prescriptions to meet the expectations of the mandate and to establish an effective program to deter prescription fraud.

THE IMPACT OF PROTECTED PRESCRIPTIONS

The reason for the legislative action is understandable. U.S. prescription fraud losses now exceed $5 billion annually. Standard Register has been working for years with prescription issuers and states to provide better protected prescriptions, and the results have been impressive. Issuers of secured prescriptions have seen significant reductions in fraudulent activity, and states where secure prescriptions have been mandated have *already* been enjoying tens of millions of dollars in fraud reduction! The state of New York, for example, eliminated over $68 million in fraud losses within six months of deploying its secure prescription program.[3] Clearly, the savings and social impact of securing prescriptions is extremely beneficial.

Standard Register®

Managing the documents you can't live without™

Unfortunately, it is the prescription issuer who typically bears the costs of providing secure prescriptions and only indirectly enjoys the financial benefits associated with the reduced fraud. However, the mandate is not something that can be ignored. Those prescription issuers who fail to comply face a wide range of consequences.

Consequences of Non-compliance

- Medicaid rejections of non-compliant prescriptions submitted for reimbursement
- Potential penalties and enforcement actions by licensing boards, Medicaid or even law enforcement
- Increased calls and interactions between pharmacies and physicians when non-compliant prescriptions are attempted to be filled
- Unfilled prescriptions when pharmacies reject non-compliant prescriptions
- Patient frustration and ill-will when prescriptions are denied due to non-compliance
- Public safety concerns and legal actions when unfulfilled prescriptions lead to medical complications
- Negative media coverage

A MINIMAL APPROACH TO COMPLIANCE

The CMS guideline seems to be a measured interpretation of the intent of the legislation. While it was possible to dictate a broad range of security technologies be introduced immediately onto written prescriptions, CMS acknowledged the difficulties many organizations will have in designing and deploying compliant prescriptions within the time available. The two-step approach requires issuers to provide some level of protection immediately, but allows an additional 13 months to implement a broader level of protection.

The requirement to provide at least one industry-recognized feature to prevent copying, modification or counterfeiting by April 1, 2008 is easy to achieve. Correspondingly, it introduces very little protection against fraud. Selecting a single feature from the list of available technologies (provided more fully later in this paper) can be accomplished in a wide manner of ways, from printing the prescriptions on an inexpensive security paper to producing the prescriptions on a laser printer.

The requirement to address all three forms of attack by October 1, 2008 provides a slightly higher level of protection but falls well short of

Defining "Tamper-Resistance"

As the Centers for Medicare and Medicaid Services (CMS) and state Medicaid directors scrambled to develop a plausible interpretation of "tamper-resistant" in the law, Standard Register was approached to offer counsel, which was provided in the form of a white paper[4] in July, 2007. In its paper, Standard Register noted that while there are multiple ways in which a user may attempt to interpret references to "tamper-resistant" in the law, the obvious intent of the language is to deter the fraud associated with tampered prescriptions. Since this fraud can be perpetrated through a variety of techniques (mimics, alterations, theft and false issuance), it is most reasonable to conclude that the intended purpose of the language is to address *all* of these forms of attack. With this understanding, we proposed the following definition:

"Tamper resistant, in the context of written Medicaid prescriptions as well as other forms of secured non-electronic prescriptions, describes the implementation of features and process controls that can measurably reduce the occurrence of prescription fraud currently experienced from theft of authentic prescriptions, false issuance of authentic prescriptions, counterfeit prescriptions, and alterations of authentic prescriptions. Written prescriptions that fail to address one or more of these known forms of fraudulent activity cannot be considered compliant with the presumed intent of the action."

The guideline CMS issued in August emphasizes security applicable to the printed prescription in the form of mimic protection (copies and counterfeits) and alteration protection. False issuance and theft, while still significant threats, are not addressed in the guideline. Presumably, these are not addressed because they are prevented primarily through secure processes and controls which cannot be ascertained through examination of the physical prescription.

addressing the problems in a manner sufficient to substantially mitigate fraud. The vaguely-worded definitions provided in the guideline "*One or more industry-recognized features designed to prevent…*" leaves the definition open to interpretation. As written, an organization might successfully argue that a prescription produced by a laser printer on a traditional basket weave security paper meets all of the requirements of the rule, having provided at least one industry-recognized feature to prevent copying, modification and counterfeiting. Yet, a criminal could acquire the same authentic looking (even identical) paper at a local office supply store and produce multiple copies of a modifiable prescription on their personal laser printer.

THE CASE FOR A MORE AGGRESSIVE APPROACH

The case for establishing a more aggressive standard for tamper resistance is compelling when you see how fraud losses have been reduced in states that have already integrated higher levels of security into their prescription pads and processes.

Prescription issuers are strongly cautioned to avoid pursuing any solution that approaches minimal compliance. While the CMS guideline was intentionally measured and modest in its reach, the guideline also encourages states to pursue more rigorous levels of protection.

"States are free to exceed the above baseline standard as to what constitutes a tamper-resistant prescription pad. States should make their own determination whether to allow pharmacists to accept an out-of-State prescription that meets the tamper-resistant requirements of another State. Several States have laws and regulations concerning mandatory, tamper-resistant prescription pad programs, which were in effect prior to the passage of section 7002(b). CMS deems that the tamper-resistant prescription pad characteristics required by these States' laws and regulations meet or exceed the baseline standard, as set forth above."[2]

The guideline, itself, notes that several states have already implemented tamper-resistant prescription programs that require stricter controls than those demanded of CMS. Additional states are pursuing programs of their own with characteristics exceeding those in the CMS baseline. Organizations that pursue minimal compliance may open themselves to further challenges. Though they may feel they are acting in good faith with the intent of the federal law, they may well find themselves compelled to again change their prescription design when their state enacts its own requirements for tamper-resistant prescriptions.

By contrast, it has been interesting to observe just how little impact this new legislative mandate has had on issuers who had already integrated a comprehensive set of security features into their prescriptions. These well-protected organizations understand the threats prescriptions face and were confident that whatever definition for tamper resistance emerged from the CMS or their own states, they would probably be compliant. Events have unfolded in just that manner.

HOW DOCUMENTS ARE ATTACKED

Before discussing the details of how to design a well-protected prescription, it seems prudent to provide a brief overview of how prescriptions are attacked. Documents are attacked in whatever manner criminals can conceive to effect gain, but most forms of document fraud fall into one of four categories. These are:

- Theft
- Alteration
- False Issuance
- Mimics

Theft is the acquisition of an original item with intent to present false information. In the case of credentials, simple presentment of the item may be sufficient (as with a credit card or a police officer's badge). However, in most cases, document theft also entails the presentation of false information on the item, as when a blank prescription is stolen, filled in and submitted.

Alteration is the addition, removal or otherwise changing the original information on an item. Alterations employ original media but the information presented has been changed. The most common forms of alteration involve:

- Ink or toner removal ("washing" or "picking") and replacement with false information
- Lifting and repositioning (cut and paste) of images on the item
- Adding unintended information to the original item to benefit the perpetrator

False Issuance involves issuing a legitimate item under false pretenses. When perpetrated by a trusted insider, this is usually embezzlement. When perpetrated by someone outside the system, it is usually misrepresentation. In either case, an undesirable individual gains access to a legitimate item.

Mimics describe representations of an original item, often carrying falsified information. In simple cases, a mimic can be a color copy, as when currency is copied and presented as authentic. In most cases, a mimic attempts to represent an original item with falsified information, as with counterfeit driver's licenses, passports and checks. In some extreme cases, a mimic bears absolutely no similarity to the original item at all, and is simply presented as a legitimate item to someone ignorant of how that item should look.

Characteristics of successful document security technologies include, but are not limited to:

1. Features that are easy to recognize yet difficult to produce or reproduce
2. Features that reveal attempts to alter the original information
3. Features that *educate* an acceptor on how to authenticate the item

HOW DOCUMENTS ARE SECURED

Introducing "security" to a document means adding certain characteristics that enable a reviewer of that item to ascertain with an acceptable level of confidence that the document and all information present upon it are in its original and intended form.

Protecting Against Theft

When protecting against theft the key is to control access to original items and to employ tools that quickly identify if and when a theft has occurred. Some effective techniques and technologies that protect items against theft include:

- Control numbers – to reveal missing items or the source of fraudulent items
- Process controls – to minimize the exposure of authentic items to loss and misuse
- Tamper-evident package seals – to warn of tampering or missing items prior to issuance
- Non-specific carton labeling – to avoid calling attention to sensitive items
- Secure handling and storage procedures

One of the few on-document technologies for protecting against theft is the control number or document ID. Without some form of unique identification for each item, there is no effective way to determine if any item is missing. However, employing unique IDs is useless unless you implement a process for tracking these IDs and recognizing when an item is missing.

Access to original items must be considered throughout the supply chain for that item. This includes, but is not limited to:

- Manufacturing (printing and production of the document)
  - Where are the materials accessible on the plant floor?
  - How is waste protected?
- Shipping
  - Is the transport secure?
  - Is it possible for items to "fall off" the truck?
- Warehousing
  - How will receipt of the entire shipment be confirmed?
  - Is the shipment secure from receipt to storage?
  - Are the items protected from unauthorized access?
- Customer acceptance
  - How will receipt of the entire shipment be confirmed?
  - Is the shipment secure from receipt to storage?
- Customer storage
  - Are the items protected from unauthorized access?
- Application fulfillment
  - Are the items protected from unauthorized access?
  - How are missing items identified and processed?
- End-user delivery
  - Is the transport secure?

Protecting Against Alteration

No later than October 1, 2008, to be considered tamper resistant, a prescription pad must contain one or more industry-recognized features designed to prevent the erasure or modification of information written on the prescription by the prescriber.

When protecting against alteration, the key is to complicate the removal of original information and to employ tools that quickly identify if and when an alteration has occurred. Some effective techniques and technologies that protect against item alterations include:

- Toner anchorage – to complicate the removal of toner
- Chemical stains – to reveal chemical eradication attempts against ink or toner
- Laid lines – to reveal cut-paste attempts on an item
- Chemical reactive inks – to reveal "washing" attacks
- Overcoatings, laminates and varnishes – to secure written content on the item
- Erasable ink backgrounds – to reveal attempts at ink and toner removal
- Borders and fill characters – to complicate attempts to add-on extra information
- On-item encodation techniques (bar codes, other patterns) – to validate item content
- Education – to enable reviewers to recognize and react to evidence of alterations

Protecting Against False Issuance

When protecting against false issuance, the key is to control access to the issuing process, allowing no one access without a clear understanding of identity, and employing tools that quickly identify if and when an item was issued under false pretenses. Some effective techniques and technologies that protect against false issuance include:

- Controlled access – to prevent unauthorized individuals from activating the issuing system
- Separation of responsibilities – to make it harder for a perpetrator to process an unauthorized activity without detection
- Teaming – assigning multiple individuals to execute tasks such as issuance and/or reconciliation to make it harder for a perpetrator to process an unauthorized activity without detection.
- Surveillance – to make it harder for a perpetrator to process an unauthorized activity without detection
- Regular audits – to instill an understanding that the crime will be detected
- Random audits – to introduce a level of uncertainty that the crime will go undetected until the perpetrator has escaped
- Education – to enable administrators to implement robust business practices and controls

Protecting Against Mimics

No later than October 1, 2008, to be considered tamper resistant, a prescription pad must contain one or more industry-recognized features designed to prevent unauthorized copying of a completed or blank prescription form, and one or more industry-recognized features designed to prevent the use of counterfeit prescription forms.

When protecting against mimics, the key is to employ tools that enable a reviewer to ascertain the legitimacy of the item and the information on it, and to educate the reviewer on how to utilize those tools. Some effective techniques and technologies that protect against mimics include:

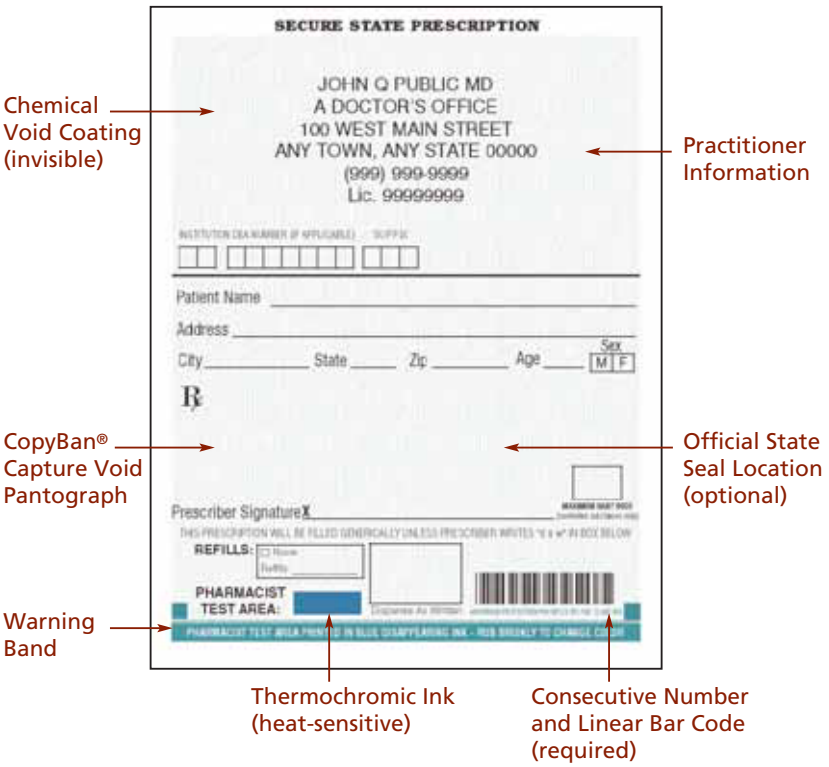
- Positive authentication systems (e.g. Positive Pay)
- Security patterns
  - Void pantographs
  - Microprinting
  - Prismatic printing
  - Lenticular patterns
  - Encodation schemes
- Security inks
  - Thermochromic inks – Inks that change color or disappear when warmed
  - Color-shifting inks – Inks that change color when view from different angles
  - Taggants – Unique compounds or markers that can be detected with special equipment
- Watermarks (including artificial) – unable to be replicated on copiers and scanners

- Intentional misprints
- Warning bands and instructions – to enable reviewers to recognize the presence or absence of authentication tools present on the item
- Exemplars – to educate pharmacists and issuers on how to verify an authentic item

BUILDING A ROBUST TAMPER-RESISTANT PRESCRIPTION

As noted in the *How are Documents Secured* section, there are a multitude of different technologies that can be applied to a prescription to protect it. When developing tamper-resistant prescriptions, Standard Register recommends protection technologies designed to address all forms of possible attack but emphasizes the need for additional protection against the two most frequently encountered methods of prescription fraud: alterations and false issuance.

A Comprehensive Solution



When recommending tamper-resistant prescription designs to our customers, Standard Register encourages the following features.

Anti-Theft

- Control numbers
- Robust production process controls
- Robust storage & handling process controls
- Regular SAS70 audits

Anti-Mimic

- Controlled safety paper
- Artificial watermark (may fluoresce)
- Copyban Capture® VOID pantograph
- Thermochromic inks
- Warning bands
- Exemplars & education

Anti-Alteration

- 3-language chemical VOID
- LaserLock® (if appropriate)
- Laid Lines
- Barcode

Anti-False Issuance

- Robust issuer controls and protocols
- Regular audits

CONCLUSION

Different vendors may promote or emphasize particular technologies due to preferred manufacturing or business needs and we will not presume to assess the overall protection provided by any vendor's proposed solutions in this paper, so long as that vendor is recommending a comprehensive set of protective features that address the full spectrum of threats the prescription is expected to encounter.

NOTES

1. P.L. 110-28, The U.S. Troop Readiness, Veterans' Care, Katrina Recovery, and Iraq Accountability Appropriations Act, 2007. In it, title 19 of the Social Security Act (42 USC 1936b(i) was amended. Specifically, section 1903b(i), paragraph (23) now states "(1) …with respect to amounts expended for medical assistance for covered outpatient drugs (as defined in section 1927(k)(2) for which the prescription was executed in written (non-electronic) form unless the prescription was executed on a tamper resistant pad".
2. SMDL #07-012. CMS Guidance on Tamper-Resistant Prescription Pads
3. "Tamper Proof Prescription Drug Pads," State of New York presentation, National Association for Medicaid Program Integrity conference, August 26-29, 2007.
4. Standard Register whitepaper: Defining a "Tamper Resistant" Prescription, July 24, 2007 response to the Centers for Medicare and Medicaid Services.

ABOUT THE AUTHOR

Dan Thaxton is a nationally recognized expert on the subject of document security technologies. He is currently active with the North American Security Products Organization (NASPO) to refine the ANSI National Security Assurance Standard. As a member of the ANSI X9-TG8 workgroup he is assisting with the development of national Check Security Guidelines. He is also a member of the board of directors of the Document Security Alliance (DSA).

Thaxton has contributed to the development of uniform U.S. Birth Certificate standard recommendations, led an industry & government team recommending security improvements to the U.S. Social Security Number card, and he has consulted with Congress and the Department of Homeland Security on document security-related topics. Thaxton has authored numerous Smart Card and document security-related patents.

As Standard Register's in-house expert on document security and fraud, Thaxton regularly speaks to banking, treasury management, payroll, and government security professionals at conferences across the country.

For more information, visit: **www.standardregister.com/securedocs**.

ABOUT STANDARD REGISTER

Standard Register (NYSE: SR) is a premier document services provider, trusted by healthcare, business and government to manage the critical documents they need to thrive in today's competitive climate. Relying on nearly 100 years of industry expertise, Lean Six Sigma methodologies and leading technologies, the company helps organizations mitigate risks, increase efficiency, reduce costs, grow revenue and meet the challenges of a changing business landscape. It offers document and label solutions, technology solutions, consulting and print supply chain services to help clients manage documents across their enterprise.

Standard Register
600 Albany Street
Dayton, OH 45408
1.800.755.6405

www.securescrip.com
Form No. 2010-POD Rev. 12/07

SR
LISTED
NYSE