THE IMPORTANCE OF ON-DOSE TECHNOLOGIES IN THE FIGHT AGAINST MISUSE, ABUSE AND ILLEGAL DIVERSION OF OPIOIDS

A WHITE PAPER

By

John Glover, DPA
President John Glover Consulting, Inc.
Vice President, Corporate Security, Bristol-Myers Squibb Company (retired)
Executive Assistant Director for Administration, Federal Bureau of Investigation (retired)
Founding Member, Pharmaceutical Security Institute

THE IMPORTANCE OF ON-DOSE TECHNOLOGIES IN THE FIGHT AGAINST MISUSE, ABUSE AND ILLEGAL DIVERSION OF OPIOIDS

By
John Glover, DPA

BACKGROUND

Opioids are regarded as safe and effective therapies for moderate to severe pain for many patients. However, opioids are subject to heightened regulation and classified by the U.S. Drug Enforcement Agency (DEA) as Schedule II or Schedule III controlled substances because of their high potential for abuse and addiction.

It is well-documented that the misuse, abuse and illegal diversion of opioid pain medications and other Schedule II controlled substances (CIIs) are reaching epidemic proportions. Drug treatment admissions for prescription painkillers have increased more than 300 percent from 1995 to 2005.[1] Recent reports indicate that nationally, more than seven million people abuse prescription drugs — more teens abuse prescription drugs than any other illicit drug, except marijuana; more than cocaine, heroin, and methamphetamine combined.[2] In addition, the number of deaths involving controlled prescription drugs, particularly opioid pain relievers (such as oxycodone, hydrocodone, methadone, morphine, and fentanyl), increased 66 percent from approximately 3,484 in 2001 to 5,789 in 2005, according to the Centers for Disease Control and Prevention (CDC).

Nationally, law enforcement reports indicate that criminal gangs have moved into the distribution and trafficking of approved CII and CIII medications.[3] Many of the same distribution channels used to transport cocaine, heroin and other street drugs now distribute approved opioids, and at times, counterfeit versions of these medications. The tracing of diverted opioid medications is nearly impossible since criminals have penetrated the legitimate supply chain to divert legitimate product to illegitimate uses and have introduced illegitimate product into the legitimate supply chain.

---

[1] *Prescription For Danger: A Report On The Troubling Trend of Prescription And Over-The - Counter Drug Abuse Among The Nation's Teens*. Office of National Drug Control Policy; January 2008.
[2] Ibid.
[3] *National Drug Threat Assessment 2009*. National Drug Intelligence Center; December 2008.

The Challenges of Illegally Diverted Opioids

The illegal diversion of opioids is a key factor in the misuse and abuse of these medications. While there are many factors that contribute to the action of illegal diversion, two key factors must be addressed if manufacturers, law enforcement, government agencies and regulators are going to make significant strides in reducing this illicit trade. The first factor is the lack of source information that can be gleaned from confiscated products following successful law enforcement activities. The second is the convoluted distribution system that allows cross-state shipping of opioid products from wholesalers to regional distribution centers, and ultimately, retail pharmacies that may or may not be in close proximity to the regional distribution center.

From a law enforcement perspective, one of the most fundamental variables in a successful investigation is the amount of information investigators have on which to base their efforts. Unfortunately, in the case of illegally diverted opioids, the information at hand is usually quite minimal given that the medication is typically repackaged from its original container and the medication itself carries no information as to the intended site of distribution. This lack of on-dose source information presents a challenge for law enforcement and government agencies seeking to initiate investigations, which in turn hampers and prolongs investigations, thereby reducing the potential for a successful outcome.

Complicating this lack of information is the fact that the distribution system for opioids does not differ materially from that of non-scheduled products. Manufacturers ship large quantities of opioids to wholesalers, who in turn ship to their regional distribution centers to meet demand. Further, the regional distribution centers in turn service retail pharmacies that may or may not be geographically close in proximity to the distribution center. Opioids path through the supply chain is quite circuitous and provides various opportunities for diversion, increasing the burden on investigators and heightening the probability of a failed investigation.

Regulatory Response

The U.S. Food and Drug Administration (FDA) is using new authority to control drug misuse by classifying it as an adverse event. In 2007, the Food and Drug Administration Amendments Act was signed into law, giving the FDA new authority to require Risk Evaluation and Mitigation Strategies (REMS) for certain drugs and biological products.[4] REMS are required to manage a known or potential serious risk associated with a product, which can include risks associated with drug abuse, overdose and withdrawal.

On September 5, 2008, the FDA released its quarterly report of drugs and their potential related side effects which are under review by the agency. Utilizing new authority, the FDA listed Oxycodone Hydrochloride Controlled-Release (OxyContin) with related side effects of misuse, abuse and overdose. [5]

On March 3, 2009, the FDA held a meeting with 16 manufacturers of opioid products to discuss a required REMS program "to ensure that the benefits of the drugs continue to outweigh the risks of: 1) use of certain opioid products in non-opioid-tolerant individuals; 2) abuse; and 3) overdose, both accidental and intentional."[6] The importance of addressing illegal diversion was underscored at this meeting by the FDA. The Agency identified diversion as a "surrogate marker" for misuse and abuse and emphasized the importance of addressing the issue in an opioid-specific REMS.

To date, REMS programs have focused on patient and prescriber education. While these elements will play an important role in an opioid-specific REMS, controlling the nefarious criminal elements, illicit diversion, and intentional misuse and abuse of opioid products will require a more specialized mitigation approach.

---

[4] 21 U.S.C. § 355(p) (2007).
[5] "Potential Signals of Serious Risks/New Safety Information Identified by the Adverse Event Reporting System (AERS), January - March 2008." Posted on the FDA web site, Sept. 5, 2008.
[6]

Industry Response

Opioid manufacturers have attempted to address the issue of illegal diversion by the use of on-package technologies such as Radio-frequency identification (RFID), which assists in the tracking of a package through the supply chain. These efforts have failed for multiple reasons including: the lack of supportive equipment and/or participation of downstream supply chain partners; the motivation of criminals to defeat traditional track and trace technologies such as RFID; and the fact that the vast majority of diverted, illicit product is not found in the original manufacturing package, but rather in plastic, zip-locked bags or other non-standard "packaging".

On their own, package securing technologies, such as RFID and other on-package technologies including serialization and 2-D barcodes, are ineffective in addressing the issue of illegal diversion, and the misuse and abuse of opioids and other CII products.

REVISED RESPONSE MUST INCLUDE ON-DOSE TECHNOLOGIES

Newly available, state-of-the-art, on-dose technologies, such as NanoEncryption™ technology developed by NanoGuardian™, can greatly assist in mitigating illicit diversion and intentional misuse and abuse by providing tracing information on each and every dose of a medication, whether in a tablet, capsule or vial form.

Dose-level tracing technology provides many benefits necessary for a successful opioid-specific REMS, including the following:

- On-dose technology does not require equipment or participation of downstream supply chain members to be effective;
- Since the technology resides on each and every dose of the medication, repackaging by criminals, as well as legitimate supply chain members, has no effect on the tracing information each dose can communicate to manufacturers, regulators, and law enforcement, thereby greatly

enhancing investigational activities and providing keen insight into the flow of illegally diverted product through the supply chain;

- The information associated with certain on-dose technologies is virtually unlimited and can include the capability to associate the drug dose with on-package technologies such as RFID, creating a parent-child relationship between packaging and the specific dose.

This White Paper details how one such on-dose technology, NanoGuardian's NanoEncryption technology, could be implemented as a key element of an opioid-specific REMS. It will also discuss the ability of NanoGuardian's NanoEncryption to meet the requirements that elements of a REMS must, including:

- Commensurate with the specific serious risk listed in the labeling of the drug;
- Not be unduly burdensome on patient access to the drug;
- Be designed to be compatible with established distribution, procurement and dispensing systems; and
- Have the ability for generic and innovator products to use a single shared system to implement the elements to assure safe use.

Employing On-Dose Technology as a Component of REMS

One goal of any diversion control system should be to ensure that at any point in the system, a products original shipping destination from the manufacturer can be obtained in a rapid, discreet manner by appropriate authorities so that a determination may be made whether the product is where it was intended - both geographically and within the supply chain.

A comprehensive, highly functioning diversion control system must include the following:

- The flexibility to run "sting" operations by manufacturers and law enforcement to identify and apprehend criminal gangs moving large volumes of diverted product;
- The ability to monitor sudden changes in purchasing patterns in regional areas; and

- Technology that does not alter the medication in any way by increasing the risk of adverse events or reducing efficacy.

Until recently, manufacturers have only had on-package technologies such as RFID to protect their brands from illegal diversion. RFID can provide two important functions; it can assist in managing and controlling inventory, and identify the intended recipient of fully-packaged products. Unfortunately, given the dynamics of opioid diversion, packaging containing an RFID chip is rarely if ever accompanying the zip-locked baggie of confiscated product. As such, the diversion "protection" and information that on-package technologies provide is limited at best.

NanoGuardian's NanoEncryption Technology

NanoGuardian's on-dose NanoEncryption technology became commercially viable within the past year and can provide a significant resource to manufacturers and law enforcement in addressing the illegal diversion of opioids. In 2008, a NanoGuardian client received approval of its Supplemental New Drug Application (SNDA) for implementing NanoEncryption technology as a brand protection initiative.

NanoGuardian's NanoEncryption technology provides on-dose layered security features at the overt, covert, and forensic level and can be applied directly to tablets, capsules and vial caps. NanoGuardian has perfected a way to impart these security features on each dose without adding any particles or chemical markers to the current product. The multi-layered security features enable NanoGuardian to provide a dual-protective benefit to manufacturers with a single technology. The overt and covert security features enable authentication at any point in the supply chain, while the forensic NanoCodes provide comprehensive tracing information on every single dose.

NanoGuardian's NanoCodes can be associated with an unlimited amount of data, including but not limited to product information (strength, expiration date), manufacturing information (location, date, batch and lot number), and distribution information (country, distributor, wholesaler, chain, RFID or 2-D Barcode). Since NanoGuardian's on-dose protection always remains with the specific dose, even after numerous repackaging efforts, NanoGuardian provides comprehensive tracing

information and brand integrity that traditional on-package and e-pedigree technologies cannot alone provide.

The unlimited dose-level information provided by NanoGuardian's NanoCodes can help address the current challenges facing law enforcement and government agencies. NanoGuardian's technology provides a crucial cornerstone to any investigation – information – and will improve the ability of all involved in the fight against illegal diversion.

NanoGuardian's program is also cost-effective at $0.005 to $0.01 per tablet/capsule NanoEncrypted, depending on volume. Compared to the devastating costs of diversion including the addiction of our youth, escalating crime related to addiction, and death from overdose; less than a penny per dose is a reasonable investment to provide a true weapon in the war against illegal diversion.

Proposed Use of NanoGuardian's NanoEncryption Technology

The on-dose distribution data contained with NanoGuardian's forensic-level NanoCodes will have significant benefit for investigators, especially when combined with a more restrictive distribution pattern for wholesalers. As such, the application of NanoEncryption technology should be employed as part of a restricted distribution scheme to provide optimal, practical control over highly diverted products. NanoGuardian's technology could be employed in the following manner:

1. Contrary to the traditional national-level wholesaler order system in use today, and in order to gain a better awareness and understanding of regional opioid distribution patterns, wholesalers must present to manufacturers forecasted opioid demand for their Regional Wholesale Distribution Centers (RWDC). Given that there are approximately 110 Regional Wholesale Distribution Centers in the U.S., a region-based distribution model will provide significantly better understanding of regional opioid ordering patterns, while having no impact on patient access to product for legitimate need.

2. After NanoEncryption, each and every opioid dose possesses a NanoCode that at the very least identifies the manufacturer's shipping date and the specific RWDC to which the product will be shipped.
3. Manufacturers ship opioid products containing the respective RWDC NanoCodes directly to the RWDC, per the forecasted demand submitted by the wholesaler.
4. RWDC receive NanoEncrypted product and are responsible for maintaining strict records of quantities distributed to retail pharmacies and other licensed health care facilities.
5. Upon a successful seizure of illegally diverted product, law enforcement and government authorities are able to determine within 24 hours via the NanoCode the RWDC of original distribution and begin to investigate within the supply chain. If a bag of opioids seized in Florida possessed a NanoCode reflective of a Florida-based RWDC, the investigation would begin evaluating the local supply chain for leaks. If on the other hand, the Florida seizure had NanoCodes reflective of product that was originally shipped to a California-based RWDC, or perhaps another country, the investigation could look for interstate or international movement of product either legitimately or illegitimately.
6. The first Product Integrity Center containing the specialized decryption equipment required to read and decrypt the NanoCodes is located at NanoGuardian's headquarters near Chicago; however, NanoGuardian has expressed a willingness to work with DEA and FDA to house the specialized decryption equipment at their respective forensic centers. Manufacturers may also have specialized equipment designed for a desired manufacturing site.

National Implementation of the NanoGuardian Diversion Control System

A solution is not a solution if it cannot be implemented, and the NanoGuardian Diversion Control System can be operational among all opioid manufacturers within the next 18 months, assuming SNDA approval is required for all dosage forms. This implementation time is reduced if CBE-30 regulatory filings are allowed by the FDA given that NanoGuardian's technology has already been the focus of an approved SNDA.

Implementation of the NanoGuardian Diversion Control System would require changes in the ordering and planning systems for manufacturers and wholesalers only (required with the move to

better visible Regional Wholesale Distribution Centers) with no changes for pharmacies, patients or prescribers.

NanoGuardian Diversion Control System National Implementation Timeline

The following timeline assumes a July 1, 2009 start date and includes all 16 branded and generic manufacturers of opioids contemplated in the REMS program. While all of the manufacturers could be ready by June 30, 2011, many manufacturers could be ready before that date. Finally, additional resources and involvement from the FDA and DEA could shorten the timelines.

Phase I – by June 30, 2011

- NanoEncryption initiated for all opioid sustained release products
- Initiate Regional Wholesale Distribution Center forecasting by wholesalers and associated product distribution by manufacturers for CII opioids
- Develop inter-agency law enforcement coordination protocols
- Develop tracking protocols for the proactive monitoring of diversion data in the marketplace

Phase II - after June 30, 2011

- Implement inter-agency law enforcement coordination protocols and diversion tracking protocols developed in Phase I
- Collect data and develop additional tactics to combat illegal diversion

Summary

The misuse and abuse of opioids and other CII-CIII medications is escalating at an alarming rate and is a growing national concern. The consequences are severe, often deadly, and at the heart is illegal diversion. While manufacturers, law enforcement and government agencies are working hard to address this concerning issue, recent trends suggest loudly that the criminals are winning the costly war of illegal diversion.

A successful outcome requires that all parties work together in addressing the issue of diversion and that the collective group embrace all available means necessary to stem the tide and begin realizing a positive impact in averting illegal diversion. These means must include on-dose tracing technologies, such as NanoGuardian's NanoEncryption technology, that provide invaluable information to investigators, despite an environment of multiple repackaging and deception. On-dose tracing technology provides law enforcement the essential source information it needs to launch successful investigations, which result in the arrest and imprisonment of those who are ultimately responsible for the misuse and abuse of opioid medications that is plaguing our country.

ABOUT THE AUTHOR - JOHN GLOVER

Dr. John Glover has a distinguished career spanning more than 35 years with the FBI, Bristol-Myers Squibb Company (NYSE: BMY), the Pharmaceutical Security Institute and the U.S. State Department's Overseas Security Advisory Council.

In March 1989, Dr. Glover retired from a distinguished career with the FBI, where he investigated, supervised and managed numerous successful high-profile investigations. During his tenure, he was designated executive assistant director for administration at FBI Headquarters in Washington, D.C., one of three direct reports to the director of the FBI.

Later, Dr. Glover served as vice president, corporate security for Bristol-Myers Squibb Company. Among his many accomplishments during this timeframe, Dr. Glover was instrumental in creating the Pharmaceutical Security Institute, an industry-wide, anti-counterfeiting body. He also served as co-chairman of the U.S. State Department's Overseas Security Advisory Council.

Today, Dr. Glover serves as president of John Glover Consulting, Inc., which provides consulting services to a very select number of prominent corporate and non-governmental entities.

Dr. Glover is also Chair of the Security Advisory Board for NanoGuardian.