Enhancing Access to Prescription Drug Monitoring Programs Using Health Information Technology:

Using Direct Messaging to Send Secure, Unsolicited Patient-at-Risk Alerts: A Pilot Study

2012

MITRE

The Office of the National Coordinator for Health Information Technology

SAMHSA

Substance Abuse and Mental Health Services Administration

DEPARTMENT OF HEALTH & HUMAN SERVICES • USA

Overview

Goal

The Indiana Direct Messaging pilot demonstrated the value of health IT connectivity by:

- Using Direct (email) messages to proactively alert providers (prescribers) of potential "at-risk" patients
- Making Prescription Drug Monitoring Program (PDMP) data more readily available while retaining information security

This pilot configuration showcased the workflow, ease of use, and added technical value of improved access to PDMP information in an ambulatory care setting by sending an unsolicited report through Direct Messaging. To achieve this:

- The PDMP generated unsolicited reports based on pre-established criteria that may indicate a patient is at-risk for drug mis-use.
- The Direct Project created a set of standards, services, and policies that provide Internet-enabled transport of patient data between known, mutually trusted participants. Appendix A addresses this technology in detail.

In addition, the pilot examined the issue of appropriate "at-risk" threshold criteria, which were used to identify patients who may be in need of additional management by care providers based on their patterns of prescriptions for controlled substances.

Pilot Design

This pilot demonstrated the added value of providing unsolicited reports for "at-risk" patients by secure electronic messaging. INSPECT, the Indiana PDMP, provided weekly Person of Interest (POI) Alerts to prescribers at ambulatory clinics based on a defined "at-risk" threshold of prescription drugs obtained by a given patient. The issue of thresholds is highly relevant to the pilot design, and Table 1 shows the list of relevant "at-risk" thresholds for INSPECT.

Table 1. Patient "At-Risk" Thresholds for INSPECT

At-Risk Threshold (exceeding)	Status
10/10/2	Current INSPECT policy
6/6/2	Approved by INSPECT Board of Directors and pilot default
3/3/2	Approved by head of INSPECT and available upon request to pilot participants

These thresholds defined the number of prescribers and pharmacies that a patient used in a given time-frame. In the pilot context, 6/6/2 means meeting or exceeding 6 prescribers or 6 pharmacies as the source of scheduled prescription drugs in a two-month (60-day) time-frame.

The pilot included three reporting cycles. INSPECT generated POI Alert reports each week and sent the messages to prescribers that had patients over the threshold. The Cerner Corporation served as the Health Internet Service Provider (HISP), providing connectivity, and also furnished the participants with a Direct-compliant inbox ("Cerner Direct inbox") for use in sending and receiving Direct messages. Appendix A addresses HISP services in detail. In some cases, multi-physician practices chose to share a single inbox for administrative simplification; this is permitted under Indiana state law. Recipients had the option of configuring a "new mail" alert message for their email box that automatically triggers upon receipt of a Direct message in their Cerner inbox to ensure that they were made aware of any new messages. Prescribers without patients over the threshold received a "no at-risk patients" message during the pilot execution period.

Appendix A describes relevant technical considerations for the pilot, including a list of participants and an example POI Alert letter. Appendices B and C discuss operational and legal considerations for the pilot, respectively. Figure 1 shows the pilot workflow.

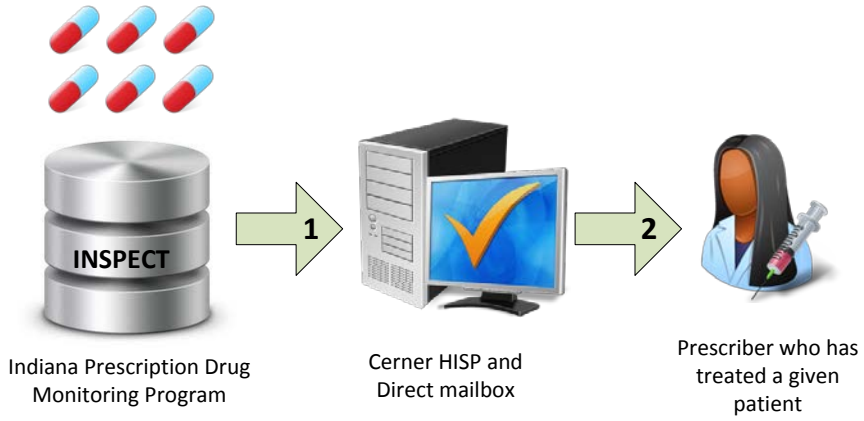

Figure 1. Pilot Workflow Diagram

Note that both sender (INSPECT Coordinator) and recipient (prescriber) of the POI Alert used the Cerner HISP, had Cerner domain names (e.g., @clinic.cernerdirect.com), and used a Cerner Direct inbox accessed on the Internet. As illustrated in Figure 1:

1. The INSPECT analysts produced a set of POI Alerts for patients who exceeded the threshold for scheduled prescription drugs and used their Cerner Direct inbox to send a message containing this alert to the ambulatory care prescribers who prescribed to that patient.

2. The prescribers who treated that patient in the threshold time-frame received these POI Alerts using their Cerner Direct inbox.

Experiment

Pre-Pilot State

POI Alerts were sent via regular email and postal mail on a weekly basis for patients who exceed the state-determined threshold. The recipients of these unsolicited reports are the prescribers who prescribed controlled substances to these patients in the threshold time-frame. Prescribers who had no patients over the allowed limit received no notice that cycle. As noted in Table 1, the pre-pilot POI Alert threshold was 10/10/2.

Hypotheses and Specific Methods

The hypotheses in Table 2 directly relate to the six areas of interest that were the basis for evaluating the effectiveness of the pilots. Appendix D describes the evaluation methods in detail.

Table 2. Evaluation Criteria

Area of Interest	Intended Impact
Ease of Use	The new, secure method for receiving POI Alerts will be as or more convenient and useful than the previous method(s) employed
Fit with Workflow	Fits within both the current physician and PDMP workflows and will not add to operational overhead
Technical Impact	POI alerts can be sent via Direct and efficiencies can be obtained for both sender and recipient
Clinical Impact	Results in greater oversight of patients, with those most in need receiving deserved attention
Driver of Adoption	Will be well accepted by the prescribers and INSPECT staff, and the pilot will serve as a springboard for continuation of use and further adoption
Optimization Factors	Has additional opportunities to improve

Results

This pilot resulted in the successful sharing of POI Alerts with providers via secure messaging, providing an opportunity to share patient information more securely…. Table 3 lists the POI Alerts disseminated during the pilot for each clinic and the threshold used.

Table 3. POI Alerts Disseminated During the Pilot

Participating Ambulatory Clinic	Prescribers	Alerts	Threshold Used
Pain Control Associates	2	50	3/3/2
Gastroenterology of Southern Indiana	4	4	6/6/2

Raj Clinics	2	5	6/6/2

It should be noted that because the reports' iteration cycle is short compared to the query time-frame (one week vs. two months), there was some probability of receiving successive weekly reports for the same patient, based on the same data. Participating prescribers who shared an inbox did not receive duplicate letters for the same patient, as these were not sent by the INSPECT team.

A total of three prescribers provided feedback, representing 38% of participating prescribers. Feedback from the INSPECT Coordinator who sent the alerts was obtained separately. Table 4 addresses the pilot results in light of the specific evaluation criteria outlined in Appendix D.

Table 4. Results

Area of Interest	Participating Prescriber Response	INSPECT Coordinator Feedback
Ease of Use	• 33% reported having received an alert by email prior to the pilot • 67% had never received one • 67% agreed that Direct is a convenient method for receiving the alert	Regular email via Microsoft Outlook was the predominant method for sending alerts, with postal mail a distant second.
Fit with Workflow	100% reported that Direct is preferable to the previous method for receiving alerts	Direct Messaging was noted as more secure, but less convenient than Microsoft Outlook. It's still a good trade-off.
Technical Impact	59 alerts were received during the pilot period by Direct Messaging	None of these 59 alerts would have been sent under the 10/10/2 threshold.
Clinical Impact	• 67% agreed that the information in the alert was sufficient for use with the patient • 33% agreed that this would help with patient management	The patient's prescription history could be sent in a secure message, which would eliminate the need to look up the patient in INSPECT.
Driver of Adoption	• 67% would recommend this to their colleagues for use in clinical data exchange • 33% would like to continue to use this for receiving alerts	Full adoption would require staffing changes or automation of the process. Still, the value of secure clinical messaging (in general) is considerable and adoption by health information exchanges (HIE) is recommended.
Optimization Factors	33% would like to see the alerts integrated within their EHR	A method for automation of bulk Direct Messaging is desirable, if used.

Discussion

The Direct inboxes and HISP services provided by Cerner were an essential part of the pilot, and were used by all participants. A comparison of the pilot implementation vs. the pre-pilot environment highlights a number of relevant points:

Direct vs. unsecured email

- Sending POI Alerts over unencrypted email cannot guarantee the security of protected health information (PHI). This precludes the inclusion of a patient's scheduled prescription drug history.
- Direct Messaging is highly secure. This would have allowed the inclusion of PHI in the message, including a full scheduled prescription drug history. This also would have made manual lookup of the patient in INSPECT unnecessary. The pilot did not include this option, but this is the next logical step, and the use of Direct is highly enabling in this regard.
- All pilot participants who provided feedback agreed that Direct was superior to regular email.

Direct vs. postal mail

- Postal mail offers the typical drawbacks of paper-based data transmission, including the lack of security and timeliness as well as significant per-unit costs.
- Electronic transmission of Direct messages is both timely and secure, and further, enables multi-office practices (e.g., Raj Clinics, which has six sites) to receive the alert regardless of daily location without duplicative effort or costs.
- Use of a shared inbox within an ambulatory practice and de-duplicating the alerts for shared patients further reduces the effort required to manage these alerts.

Participants also noted a number of tradeoffs for this specific pilot configuration:

- The identity verification needed to claim a Direct domain took considerable time and effort due to the extensive required identity verification documentation (see Appendix A). This is consistent with the DirectTrust requirements (http://www.directtrust.org/). Improvements in the ease of accomplishing this goal could have a major impact on user-friendliness.
- There were also delays in claiming inboxes after domain registration, and Cerner noted this as typical for new users. This also necessitated delayed delivery of some alerts in the first week of the pilot.
- INSPECT staff are more easily able to send the volume of necessary emails through Outlook than through the Cerner inbox if fully reliant on manual processes. Automation could address this.

Appropriate "at-risk" thresholds for patients also played an important role in the pilot, though this was not the main focus of the project's efforts. Note the following observations:

- Use of the 6/6/2 threshold was necessary for successfully pursuing the pilot, as none of the alerts sent would have been triggered under the current 10/10/2 threshold.
- It seems probable that a 3/3/2 threshold shows a substantial false positive rate based on discussions with the INSPECT data team. A full analysis of this topic is out of scope, but appropriate policies for setting thresholds remains an important area of investigation.
- Incremental reduction of the "at-risk" threshold over time is a marker of the continuing progress that Indiana has made in reducing abuse, misuse, and diversion of prescription drugs.

Finally, the pilot's efforts to complete the certificate exchange to establish HISP-to-HISP connectivity between Cerner and the Michiana Health Information Network (MHIN) were quite substantial, but the process could not be completed during the project time-frame. Thus, a fourth clinical practice, Urology Associates of South Bend, was unable to participate in the pilot. Still, these two parties have agreed to continue to work towards establishing trust in a logical time-frame, ideally by the end of September 2012, following a preliminary but formal DirectTrust.org attestation process. The value of this connectivity to health information exchange in Indiana in general could be considerable, as it would make all prescribers on that network immediately available for receipt of POI Alerts through Direct Messaging.

Outcome and Next Steps

The Cerner Direct inboxes remain in place for INSPECT and the prescribers at present, though further study will be needed to optimize their use for POI Alert dissemination. In response to feedback from the pilot and other customers, Cerner is in the process of incrementally rolling out a new identity verification process, which should alleviate delays in claiming domain addresses. Cerner and MHIN will continue to progress towards HISP-to-HISP connectivity.

Other Pilots

The Enhancing Access to PDMP project conducted five additional pilots in Fiscal Year 2012 which are available for review. The pilots encompass a variety of user groups, including dispensers (pharmacists) and prescribers (ambulatory and emergency department) as well as different technological solutions. These papers can be found at the Office of the National Coordinator for Health Information Technology (ONC) PDMP website: http://healthit.hhs.gov/portal/server.pt?open =512&mode=2&objID=3870.

Appendix A. Technical Considerations

The following sections contain a detailed description of the pilot design, including participants and technologies.

Participants

The following parties participated in the pilot:

- **Cerner Corporation** (http://www.cerner.com) – A large technology vendor that provides Health IT services and products to improve the efficiency of healthcare delivery, located in North Kansas City, MO. This organization provided the Direct Protocol Messaging capability for the pilot, including HISP services and a web-based inbox for sending and receiving Direct messages.
- **INSPECT (Indiana Scheduled Prescription Electronic Collection and Tracking** (http://www.in.gov/pla/inspect) – The Indiana PDMP, operated by the Indiana Board of Pharmacy, itself part of the Indiana Professional Licensing Agency. The program is based in Indianapolis, IN.
- **Pain Control Associates, LLC** (http://spinepaindoctors.com) – An outpatient ambulatory practice specializing in comprehensive pain intervention and management, located in Crown Point, IN.
- **Raj Clinics** (http://www.rajclinics.com) – An outpatient psychiatric practice that provides substance abuse management treatment at multiple sites throughout the state, including Indianapolis, IN.
- **Gastroenterology of Southern Indiana** (http://www.gsi-sie.com) – An outpatient ambulatory practice focusing on digestive conditions and procedures, located in New Albany, IN.

More peripheral pilot participants include the following:

- **Michiana Health Information Network** (MHIN, http://www.mhin.com) – A health information exchange (HIE) and healthcare IT company serving medical providers and institutions in the "Michiana" geographic area consisting of southwestern Michigan and northwestern Indiana. MHIN headquarters are in South Bend, IN. MHIN planned to participate in the HISP-to-HISP connectivity during the execution phase, but the timeline was too aggressive to permit this. Cerner and MHIN continue to work towards this goal and have agreed to establish trust following a preliminary directrust.org attestation process.
- **Urology Associates of South Bend** (http://www.apom.com/locations/urology-associates-of-south-bend) – An outpatient ambulatory practice specializing in the medical and surgical treatment of urinary tract issues, located in South Bend, IN. Their participation was through the MHIN-Cerner HISP-to-HISP connection as this practice has access to a form of Direct Messaging through MHIN. Urology Associates of South Bend

would have received POI Alert messages (three in the first cycle) if this connectivity had been enabled during the pilot.

The pilot project staff also wishes to thank the Indiana Family and Social Services Administration (http://www.in.gov/fssa), which provided helpful guidance and input.

Relevant Technologies and Tools

The following technologies and tools were vital components of the pilot.

Direct

The Direct Project, sponsored by the ONC, created a set of standards, services, and policies that enable Internet transport of health data between known participants in support of ONC's meaningful use requirements. The Project was designed to augment other means of health data exchange and to be easily adopted by entities with a variety of technological sophistication. Note that Direct does not specify an exchange format and thus does not directly address interoperability. It relies on well-established Internet technologies (e.g., S/MIME) and seeks to supplant slow, inconvenient, and/or expensive methods of health data exchange. Its use of encryption (for security) and signing (for non-repudiation) are simple, secure, standards-based, and scalable. Direct Messaging requires the use of one or more HISPs to serve as the transmission infrastructure. Reference implementations are available, and many entities provide the necessary capabilities to engage in Direct Messaging, including Cerner Corporation, which provided the web-based Direct inbox system used in the pilot.

The Cerner Direct tool is delivered through a secure webpage, rather than a desktop application, making it easier for participants with a variety of technical sophistication levels to utilize. Each Cerner domain (e.g., @clinic.cernerdirect.com) has an account administrator who is authorized to grant email boxes to persons of their choosing, but retains responsibility for ensuring that these individuals are eligible and trusted. http://statehieresources.org/wp-content/uploads/2010/12/Direct_Project_FAQs_Website.pdf

Health Internet Service Provider (HISP)

A HISP supports the connectivity required for Direct Messaging. The HISP provides its users with an infrastructure that can manage message encryption, the "circles of trust" as to who can be communicated with, and the incorporation of appropriate policies and procedures necessary to ensure a level of confidence in provisioning members on the network appropriate to healthcare. The HISP model is essentially the same as the Internet Service Providers (ISP) model, and both use many of the same protocols for message transport. However, typical ISPs do not use the necessary security processes to satisfy Health Insurance Portability and Accountability Act (HIPAA) rules regarding electronic exchange of PHI data. For example, HISPs provide for authentication of senders and receivers at the time of transport as part of the trust relationship. Likewise, digital certificates are exchanged at the time data are encrypted to establish trust. Each HISP may set its own minimal set of authentication protocols for client

applications, and each may decide whether any other HISP also meets these and is thus a potential partner for exchange (HISP-to-HISP).

During this pilot, Cerner performed the role of a "full service HISP," meaning that Cerner also took on the following responsibilities, detailed in Figure A-1:

- **Registration Authority (RA)** – Collects and verifies identity information from Direct exchange subscribers using procedures that implement the identity validation policies. The RA creates certificate signing requests (CSR) for submission to a CA. RA entities must utilize identity validation policies defined in the relevant certificate policy.
- **Certificate Authority (CA)** – An entity that signs CSRs and issues public key X.509 certificates to Direct exchange organizational or individual subscribers. A CA must create a Certification Practices Statement (CPS) that conforms to the policies.

  Every endpoint in Direct has an X509 certificate associated with it. A certificate is an electronic type of credential, meaning it can be used to unambiguously identify an entity within a certain level of assurance. Level of assurance describes the policies and procedures used to identity-proof the entity. The higher the level of assurance, the higher the level of proof that is needed to validate the entity's identity. In X509 certificates, an attribute called a certificate policy asserts levels of assurance. An object identifier (OID) uniquely identifies each certificate policy.

  Certificate management refers to the policy and procedures used to manage the lifecycle of a certificate. These include issuance, revocation, renewal, and rekeying. Certificate management can also refer to the procedures used to protect the integrity of the Public Key Infrastructure (PKI). This mainly covers protecting private keys, backing up keys, and auditing access to keys. Many of these procedures are outlined in a CPS and handled by the certificate authority. In the case of HISPs, issued certificates and their keys are held by the HISP, not the actual entities. This is a slightly different model that of from most PKIs, where the entities hold their own certificates and private keys. Because the HISP is the steward of the keys, it must take proper care in managing and protecting keys from unauthorized access or malicious attacks.

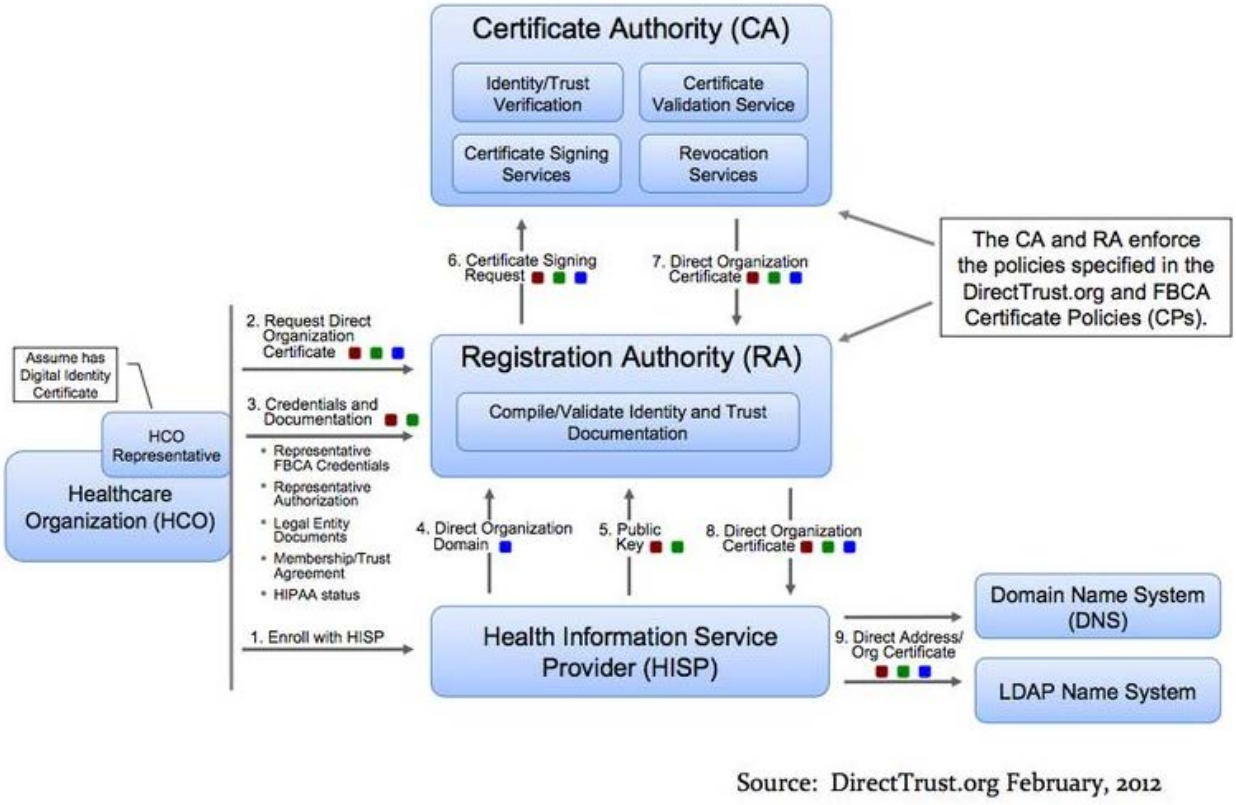

Figure A-1. Direct Identity, Trust, and Address Provisioning

Testing and Deployment Issues

Since no *de novo* development was performed during this pilot—simply deployment of existing tools—this topic is not applicable. The pilot did not encounter any deployment issues beyond what was mentioned in the discussion section.

User Interface

The Cerner Inbox tool operates in many ways simply as a much more secure email system; however, it also has a variety of value-added features, including fixed and indexable fields for patient information. Figures A-2 and A-3 illustrate the look and feel of the Cerner tool used in the pilot.

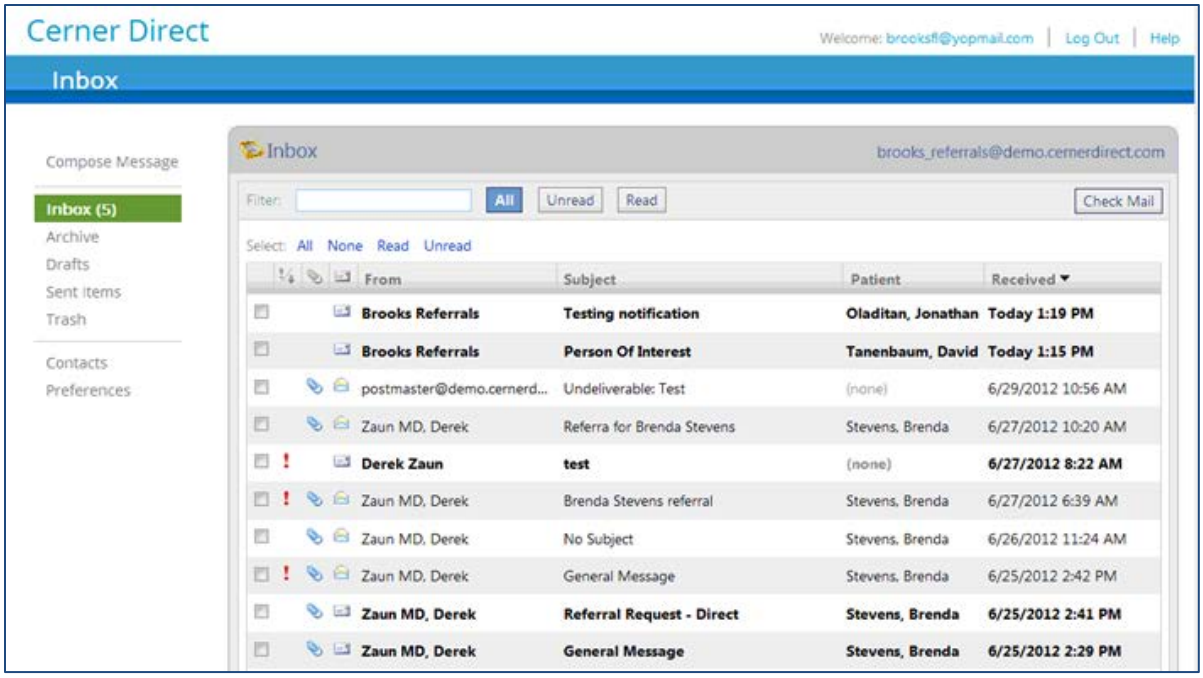

Figure A-2. Cerner Direct Inbox

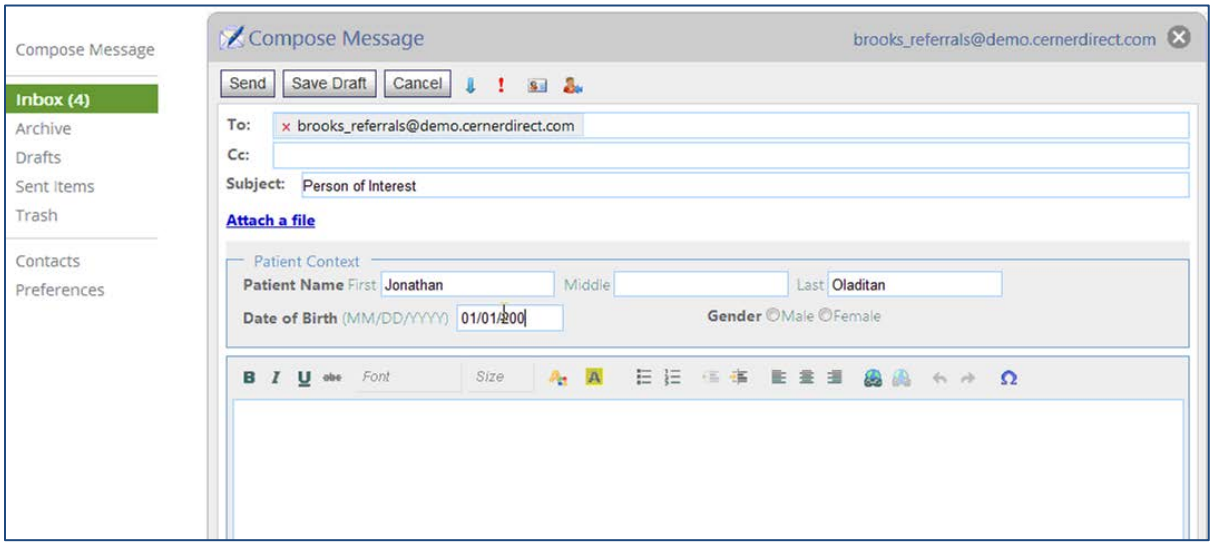

Figure A-3. Cerner Direct Email, with "Patient Context" Fields

Example Inspect POI Alert Letter

PRACTITIONER,

You are in receipt of an INSPECT Person of Interest Alert. The INSPECT Program has identified "DUMMY" as having exceeded specific patient dispensing guidelines set forth by the Indiana Board of Pharmacy. Please review the attached letter sent with this email. To review a full patient report corresponding to this patient, please submit a request through the INSPECT PMP WebCenter. If you are not currently a registered INSPECT accountholder, you may register for account access by visiting www.IN.gov/inspect.

WHAT IS INSPECT?

Since 2007 the Indiana Scheduled Prescription Electronic Collection and Tracking Program, better known as INSPECT, has sought to provide Indiana health care providers with timely controlled substance treatment information for those patients to whom they are providing treatment. All individuals with the authority to prescribe or dispense controlled substances are eligible to utilize INSPECT's web-based software, known as the PMP WebCenter, to access patient report information 24/7.

WHAT IS A PERSON OF INTEREST ALERT?

Effective July 1, 2010 the scope of INSPECT services has expanded to include a new "unsolicited report" offering in the form of Person of Interest Alerts. The Person of Interest Alert is designed to notify both registered INSPECT users and non -users alike of possible patient misuse or diversion of controlled substances. Receipt of such an alert means that -based on an objective review of available INSPECT records-a patient under your care (and potentially under the care of several other practitioners) has exceeded the patient dispensing guidelines established in August 2010 by the Indiana Board of Pharmacy.

Person of Interest Alerts should not be construed as evidence that a crime has taken place. All information contained in the INSPECT report comes from data reported to INSPECT by licensed dispensing pharmacies, and should be fully-validated to ensure that the data is accurate and complete. And so, while there is a chance that the patient's INSPECT report may not be fully complete or accurate, or that it may be flawed in other ways, in the interest of helping to limit

the illicit diversion of prescription drugs statewide, and in the interest of protecting the safety and well-being of patients, we are statutorily required to inform you of our findings.

WHAT TO DO NEXT?

If you would like to review the patient's full prescriptive history, you must first establish an INSPECT account. For more information, please visit www.IN.gov/inspect. Once you have fully reviewed the patient's prescriptive history available through INSPECT, how you proceed in handling the matter is entirely up to you, and the optimal response may vary depending circumstances /context of the situation. For additional guidance or best practices, it may be helpful for you to review your organization's policy/procedures, contact the appropriate licensing board for your profession, or seek counsel from your statewide membership association.

In weighing your options, however, please aware that the also-recently-passed IC-35-48-7-11.1 (h) states that, "A practitioner who in good faith discloses information based on a report from the INSPECT program to a law enforcement agency is immune from criminal or civil liability." Hence, if you have reason to believe that a patient's INSPECT report suggests criminal behavior on the part of the patient, you have the option of sharing your findings with a law enforcement officer.

Sincerely,

INSPECT Administrators

Various Aliases and Addresses Used by Subject:

DUMMY A 05/05/1927 715 S. BALDWIN

DUMMY DUMMY 05/14/1945 1405 N PARK AVE

DUMMY DUMMY 13 W JACKSON ST

DUMMY FILE 01/01/1901 800 Fulton St

DUMMY IMA 02/01/1901 123 MAIN STREET

Cerner Identity Verification Form for Providers

Identity Verification Form

DECLARATION UNDER PENALTY OF PERJURY MADE BY THE SUBSCRIBER TO CERNER CORPORATION.

Information below must match the records in the National Plan and Provider Enumeration System (NPPES).

Subscriber Organization Legal Business Name (LBN) _____
Subscriber Organization National Provider Identifier (NPI) _____

Business Mailing Address	Business Practice Location Address
_____	_____
_____	_____
_____	_____

Subscriber Organization Requested Direct Email Domain: @_____

I, _____ (legal name), the undersigned Cerner Direct Administrator, declare under penalty of perjury the following:

1. That the documents I have provided to the notary to substantiate the aforesaid information constitutes accurate personal information about me;
2. That I am the person referenced in the documents provided herein;
3. That I have provided the following documents to a notary as required by Cerner Corporation.

REQUIRED DOCUMENTS:

- Driver's License for Cerner Direct Administrator
- Second form of identification for Cerner Direct Administrator (not required to be a photo I.D.)
- State Sales Tax/Business license for Subscriber Organization

Cerner Direct Administrator Designation

Name of Cerner Direct Administrator _____

Contact Information of Cerner Direct Administrator:

Primary Phone _____

Secondary Phone _____

Email _____

Duties of the Cerner Direct Administrator are:

1. To verify the identity of each End User and their authority to send messages through Cerner Direct;
2. To promptly remove access when End Users leave their practice or organization, or should otherwise have their access to Cerner Direct revoked;
3. To be the primary contact to Cerner Direct Operations for any problems or questions;
4. To notify Cerner Direct Operations of any change in the named Cerner Direct Administrator above;
5. To ensure End Users comply with all state and federal laws concerning the confidentiality of personally identifiable information;
6. To ensure that End Users receive instruction regarding use of Cerner Direct for approved purposes only;
7. To promptly report any suspected abuse or misuse of Cerner Direct to Cerner Direct Operations;
8. To ensure that End Users agree to hold any user names, passwords, and any other means for accessing Cerner Direct, in a confidential manner and to disclose them to no other individual; and
9. To ensure that End Users agree and understand that their failure to comply with the Cerner Direct Terms of Use may result in termination of access to Cerner Direct.

The above named Subscriber Organization is a HIPAA covered entity or business associate, or is a healthcare related organization which treats protected health information with privacy and security protections that are equivalent to those required by HIPAA.

I, as the above named Cerner Direct Administrator possess the authorization to act in the name of the Subscriber Organization.

CERNER DIRECT ADMINISTRATOR SIGNATURE

Signed on this _____ day of _____, _____, under penalty of perjury before a commissioned Notary

_____

Cerner Direct Administrator Signature

NOTARY SIGNATURE

I, _____, a commissioned Notary hereby declare under penalty of perjury that:

1. I have read/examined the documents provided above, including their authenticity in having been properly issued by the claimed issuing authority and valid at the time of application;
2. I have substantiated with those documents and photographic image the facts set forth above;
3. I have examined the undersigned Cerner Direct Administrator under oath;
4. I have ascertained by examination of the Cerner Direct Administrator under oath that the Cerner Direct Administrator is the person referenced in the documents and the Cerner Direct Administrator is the signatory of this Declaration.

Signed on this _____ day of _____, _____, under penalty of perjury before me

_____ a commissioned Notary

_____
Notary

My Commission Expires on: _____

SUBMITTING THIS DOCUMENT

Notary: Please make copy of Driver's and Sales Tax/Business License

Mail or hand-deliver the original signed and notarized form with the copy of the verified Driver's and Sales Tax/Business License to the following address:

Cerner Corporation
Attn: Cerner Direct Operations
2800 Rockcreek Parkway
Kansas City, MO 64117

If requested, send electronic version of document to one of the following:

Fax: (816) 936-8379

Email: cernerdirect@cerner.com

Cerner Identity Verification Form for State Entities or Healthcare Stakeholders

Identity Verification Form By EIN

DECLARATION UNDER PENALTY OF PERJURY MADE BY THE SUBSCRIBER TO CERNER CORPORATION.
Subscriber Organization Legal Business Name (LBN) _____
Subscriber Organization Employer Identification Number (EIN)
_____
Business Mailing Address Business Practice Location Address
_____ _____
_____ _____
_____ _____
Subscriber Organization Requested Direct Email Domain: @_____

I, _____ (legal name), the undersigned Cerner Direct Administrator, declare under penalty of perjury the following:

1. That the documents I have provided to the notary to substantiate the aforesaid information constitutes accurate personal information about me;
2. That I am the person referenced in the documents provided herein;
3. That I have provided the following documents to a notary as required by Cerner Corporation.

REQUIRED DOCUMENTS:

- Driver's License for Cerner Direct Administrator
- Second form of identification for Cerner Direct Administrator (not required to be a photo I.D.)
- State Sales Tax/Business license for Subscriber Organization

Cerner Direct Administrator Designation

Name of Cerner Direct Administrator _____

Contact Information of Cerner Direct Administrator:
Primary Phone _____

Secondary Phone _____

Email _____

Duties of the Cerner Direct Administrator are:

1. To verify the identity of each End User and their authority to send messages through Cerner Direct;
2. To promptly remove access when End Users leave their practice or organization, or should otherwise have their access to the Cerner Direct revoked;
3. To be the primary contact to Cerner Direct Operations for any problems or questions;
4. To notify Cerner Direct Operations of any change in the named Cerner Direct Administrator above;
5. To ensure End Users comply with all state and federal laws concerning the confidentiality of personally identifiable information;
6. To ensure that End Users receive instruction regarding use of the Cerner Direct for approved purposes only;
7. To promptly report any suspected abuse or misuse of Cerner Direct to Cerner Direct Operations;
8. To ensure that End Users agree to hold any user names, passwords, and any other means for accessing Cerner Direct, in a confidential manner and to disclose them to no other individual; and
9. To ensure that End Users agree and understand that their failure to comply with the Cerner Direct Terms of Use may result in termination of access to Cerner Direct.

The above named Subscriber Organization is a HIPAA covered entity or business associate, or is a healthcare related organization which treats protected health information with privacy and security protections that are equivalent to those required by HIPAA.

I, as the above named Cerner Direct Administrator possess the authorization to act in the name of the Subscriber Organization.

CERNER DIRECT ADMINISTRATOR SIGNATURE

Signed on this _____ day of _____, _____, under penalty of perjury before a commissioned Notary

_____
Cerner Direct Administrator Signature

NOTARY SIGNATURE

I, _____, a commissioned Notary hereby declare under penalty of perjury that:

1. I have read/examined the documents provided above, including their authenticity in having been properly issued by the claimed issuing authority and valid at the time of application;
2. I have substantiated with those documents and photographic image the facts set forth above;
3. I have examined the undersigned Cerner Direct Administrator under oath;
4. I have ascertained by examination of the Cerner Direct Administrator under oath that the Cerner Direct Administrator is the person referenced in the documents and the Cerner Direct Administrator is the signatory of this Declaration.

Signed on this _____ day of _____, _____, under penalty of perjury before me

_____ a commissioned Notary

_____
Notary

My Commission Expires on: _____

SUBMITTING THIS DOCUMENT

Notary: Please make copy of Driver's and Sales Tax/Business License

Mail or hand-deliver the original signed and notarized form with the copy of the verified Driver's and Sales Tax/Business License to the following address:

Cerner Corporation
Attn: Cerner Direct Operations
2800 Rockcreek Parkway
Kansas City, MO 64117

If requested, send electronic version of document to one of the following:

Fax: (816) 936-8379
Email: cernerdirect@cerner.com

Appendix B. Operational Considerations

Key Operational Assumptions

- Cerner Corporation can provide the Direct mailboxes, HISP services, and training needed to successfully execute the pilot.
- Pilot will be limited to 3 ambulatory clinics of a total of 12 prescribers. Not all may choose to participate.
- INSPECT will only send data to prescribers in the State of Indiana, precluding interstate issues.
- There will be an adequate number of alert-worthy patients during the execution phase.
- The Indiana Professional Licensing Agency will agree to all aspects of the pilot design.
- Consistent with the recommendations of the Business Agreements for Intermediaries Work Group, Business Associate Agreements (BAA) will be sufficient for conducting the pilot project. If not, the necessary agreements will not be overly difficult to craft or negotiate.
- Cerner Corporation and the Michiana Health Information Network (MHIN) can achieve the technical, legal, and logistical agreements needed to engage in HISP-to-HISP exchange in the time available, enabling Dr. DePauw of Urology of South Bend to participate (**not met**).
- INSPECT data is available for “practitioners” who provide medical or pharmaceutical treatment, or evaluate the need for providing such treatment, to a patient. Indiana Code 35-48-7-5.8 defines a practitioner as, "…a Physician, Dentist, Veterinarians, Podiatrists, Nurse Practitioners, Scientific Investigators, Pharmacists, or any other institution or individual licensed, registered, or otherwise permitted to distribute, dispense or conduct research with respect to, or administer a controlled substance in the course of professional practice or research in the United States.”
- Sharing of Direct inboxes is permitted under Indiana law, based on appropriate delegation (e.g., physician to staff, or between physicians within a practice).

Operational Advantages or Barriers

The State of Indiana was very accommodating of all requests made during the pilot and was a key factor in the project’s success. In particular, INSPECT staff were absolutely critical for the recipient recruitment efforts, logging more than 70 phone calls and more than 500 emails to attract the participant cohort. Pharmacies in Indiana must report their dispensations to INSPECT every seven days, so the data is reasonably current and reliable.

This pilot involved a large number of participating PDMP data recipient organizations, with a variety of degrees of technical sophistication and scheduling needs. Many participating prescribers had limited or no exposure to Direct Messaging. HISP-to-HISP connectivity is difficult to achieve (policy and agreement-wise, not technically) and remains a significant

ongoing issue for the Direct community as a whole. It was noted that grant funding for INSPECT relies on metrics such as number of queries, which might be adversely affected by a highly proactive unsolicited alert system delivering the PDMP data to prescribers.

Pilot Schedule

Task Name	Start	Finish	Duration
Planning	June 11, 2012	June 29, 2012	15 days
Deployment/Training	July 2, 2012	August 10, 2012	30 days
Execution/Monitoring	August 13, 2012	August 27, 2012	11 days (3 cycles)
Post-Pilot Analysis/Report	August 28, 2012	August 31, 2012	4 days

Pilot Costs

Vendor	Services	Subcontract
Cerner	Direct Messaging HISP services and inbox, training, monitoring, reporting	$20,000

MITRE subcontracts are fixed price instruments. It is noted that no participants requested legal review costs for business (e.g., MITRE subcontract) and privacy-protection purposes. Other expenses also may have been insufficiently enumerated in this list (e.g., the many activities done by INSPECT), and regional cost factors may likewise play a role in the quoted prices. Thus, the actual cost of reproducing this pilot elsewhere may be more or less than this amount, even when attempting to exactly replicate these circumstances.

Appendix C. Legal Considerations

This section looks at the pilot's policy and regulatory considerations and obstacles, as well as the agreements implemented.

Policy and Regulatory Considerations

To successfully conduct the pilot on production systems, certain laws and policies need to be in place to support the pilot design. The following considerations were most applicable to this pilot:

- INSPECT considers the contents of the current POI Alert letter not to be PHI, even with date of birth included, as this information easily can be acquired online.
- More complete clinical information (i.e., full scheduled medication history) can be sent in a Direct message, and perhaps will be in some future iteration.
- INSPECT declined to require a BAA with Cerner, and no legal agreements of any kind were signed during the pilot period (except the subcontract between MITRE and Cerner).
- Cerner has extensive proof requirements for establishing the domain administrator for each domain; this administrator has the responsibility to ensure that accounts (email addresses) are only granted to appropriate parties. This is expected as part of the Direct HISP policy.
- Trust establishment between HISPs requires extensive requirements for trust attestation.
- Only physicians will access these alerts; no office staff will perform this role.

Other policy and regulatory details are available at the following locations: http://www.in.gov/pla/2336.htm and http://iot.custhelp.com/app/answers/detail/a_id/1206.

Appendix D. Evaluation Methods

Evaluation Approach – Hypotheses and Specific Methods

The Federal Government and the MITRE Corporation conducted pilot studies, small-scale experiments, to test the feasibility of proposed workflows and evaluate their outcomes before investing resources in a full-scale, permanent implementation. These pilots provide valuable insights concerning time requirements, system challenges, and opportunities for process improvement—all of which can be addressed to improve final system design and performance success.

Evaluating the PDMP Pilots required a disciplined and consistent approach to examine the impact of the new or changed technical and clinical work process features toward achieving the following goals:

- **Workflow Logistics** – Providing the correct amount of the appropriate information, in the proper condition, at the right place and time, in the necessary position/sequence
- **System Performance** – Achieving desired outcomes
- **Predicting Implementation Success** – Extrapolating the results to a larger system

MITRE's systematic analytic approach effectively consolidated these objectives into a set of three consistent evaluation themes: usability, impact, and scalability. The PDMP Pilots varied from simple to more complex health IT connectivity configurations to the PDMP, so testing afforded the opportunity to examine the different facets of performance along a continuum of technical sophistication (see Figure D-1).

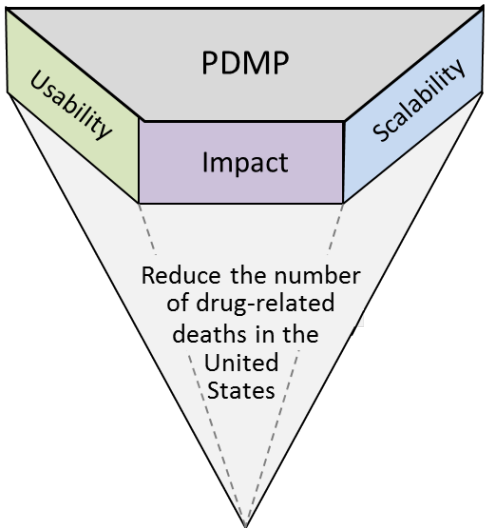

Figure D-1. Evaluation Themes

This appendix describes the three evaluation themes in detail. Each theme and its accompanying areas of interest, with associated evaluation metrics, were the basis for evaluation of the PDMP pilots.

Usability

The primary focus of the usability theme is the user's perspective. The following areas of interest concern the optimization of the care delivery experience and the efficiency in performing work processes by leveraging and maximizing technical integration:

- **Ease of Use** – Promoting easier and more efficient ways to access to the PDMP prescription drug data than the previous method for providers and dispensers
- **Fit with Workflow** – Natural integration into existing clinical and health IT workflows for providers and dispensers

Table D-1. Usability Analysis Features

Area of Interest	Evaluation Metrics	Data Source
Ease of Use	% reporting PDMP data now easier to access (pilot versus prior methods)	Participant Feedback (Solicited Response, Interview)
	Distribution of previous methods used to access data	Participant Feedback (Solicited Response, Interview)
Fit with Workflow	% indicating access to PDMP data was better than alternative option	Participant Feedback (Solicited Response, Interview)

Impact

The impact theme is meant to validate that the connectivity method to the PDMP was achieved and ultimately resulted in a positive impact to clinical care outcomes (reducing the number of prescription drug-related deaths). The following areas of interest assess the technical and clinical impact:

- **Technical Impact** – Resulted in maximizing connections to existing technologies and increased queries to the PDMP data
- **Clinical Impact** – Resulted in timely and meaningful PDMP prescription drug information, readily available at the time of decision-making, that positively impacted care delivery to the patient

Table D-2. Impact Analysis Features

Area of Interest	Evaluation Metrics	Data Source
Technical Impact	Number of unsolicited reports sent via Direct	Logged System Data
Clinical Impact	% satisfied with data provided in pilot configuration for clinical use	Participant Feedback (Solicited Response, Interview)

	% reporting change in treatment as result of better PDMP access	Participant Feedback (Solicited Response, Interview)

Scalability

The scalability theme assessed the capability of the new work processes to be widely applied and accommodate growth in the existing system of providers and dispensers. The following areas of interest assessed how well the participants adopted the new process and the degree to which it improved the existing workflow:

- **Driver of Adoption** – Accepted by the participants so that the pilot drove further adoption by other sites or user groups (e.g., providers), if applicable
- **Optimization Factors** – Generated identifiable improvement opportunities to increase the usefulness and timely availability of PDMP prescription drug information

Table D-3. Scalability Analysis Features

Area of Interest	Evaluation Metrics	Data Source
Driver of Adoption	% wishing to continue to use the new process	Participant Feedback (Solicited Response, Interview)
	% willing to recommend the new process to their peers or colleagues	Participant Feedback (Solicited Response, Interview)
Optimization Factors	% able to identify specific, actionable steps to further refine process	Participant Feedback (Solicited Response, Interview)
	Distribution of specific suggestions for improvement	Participant Feedback (Solicited Response, Interview)

Instrument for Collecting Participant Feedback

Figure D-2 shows the instrument used for collecting feedback. The survey was administered online and is available at: http://www.surveymonkey.com/s/BLP77ZL

Indiana Unsolicited Alert Pilot Survey

Exit this survey

Thank you for your participation in the Direct Protocol Messaging pilot, one jointly sponsored by the Office of the National Coordinator for Health IT (ONC) and the Substance Abuse and Mental Health Services Administration (SAMHSA), and conducted with the cooperation of the Indiana Scheduled Prescription Electronic Collection and Tracking (INSPECT).

The Direct Protocol is a secure messaging system which allows safe and easy exchange of Protected Health Information (PHI) between known, authorized users. This pilot was designed to test the utility of this type of messaging to provide access to unsolicited Person of Interest (POI) Alerts to ambulatory practitioners in Indiana. It explicitly seeks to address the utility of this approach as compared to other delivery channels used for this purpose.

Please complete the following survey to the best of your ability regarding your experience during the pilot.

1. Before the pilot, I received POI Alerts from INSPECT by:

- Email
- Postal Mail
- FAX
- This is the first POI Alert I have received

Other (please specify)

2. I found Direct Protocol Messaging a convenient way to receive POI Alerts from INSPECT

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

3. I prefer this new method for POI Alert delivery to the method I used prior to the pilot

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

4. I would like to continue to use Direct Protocol Messaging to receive these alerts

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

5. I would like to explore additional uses of Direct Protocol Messaging within my clinical practice

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

I would like to explore the following other uses

6. I would prefer to use Direct Protocol Messaging as an integrated part of my Electronic Medical Records (EMR) system

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

My current EMR is (provider/brand)

7. The amount of information provided in the POI Alert was sufficient for me for use with my patient

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

I would prefer that the following additional information appear in the POI Alert

8. Receiving these alerts electronically will help me better manage my patients

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

9. I would recommend to my colleagues that they consider adopting this messaging method for clinical data exchange

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

Specialty of colleague(s) to whom you would recommend this tool

10. Please make any additional comments

Done

Powered by SurveyMonkey
Check out our sample surveys and create your own now!

Figure D-2. Pilot Feedback Instrument

Acronyms

BAA	Business Associate Agreement
CA	Certificate Authority
CPS	Certification Practices Statement
CSR	Certificate Signing Request
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act of 1996
HISP	Health Internet Service Provider
INSPECT	Indiana Scheduled Prescription Electronic Collection and Tracking Program
ISP	Internet Service Provider
MHIN	Michiana Health Information Network
OID	Object Identifier
ONC	Office of the National Coordinator for Health Information Technology
PDMP	Prescription Drug Monitoring Program
PHI	Protected Health Information
PKI	Public Key Infrastructure
POI	Person of Interest
RA	Registration Authority