 Interstate Commission for Juveniles	Opinion Number: 01-2014	Page Number: 1
<p style="text-align: center;">ICJ Advisory Opinion Issued by: Executive Director: Ashley H. Lippert Chief Legal Counsel: Richard L. Masters</p>		
Description: The Health Insurance Portability and Accountability Act (HIPAA) as it relates to youth and family information.	Dated: January 23, 2014	

Background:

Pursuant to Commission Rule 9-101(3), the State of Rhode Island has requested an advisory opinion regarding the requirements of the Compact and ICJ Rules on the following issue:

Issues:

The State of Rhode Island is requesting clarification on the application of the Health Insurance Portability and Accountability Act (HIPAA) as it relates to youth and family information shared through ICJ. Specifically, Rhode Island asks the following:

1. Does the Juvenile Interstate Data System (JIDS) satisfy HIPAA as it relates to both Personal Identifiable Information (PII) as well as Personal Health Information (PHI)?
2. How can the same information be protected in emails from state to state? Because JIDS is a document management system, requiring the majority of state's communication to be completed through email, if there is an exemption, how would it apply generally and how would it apply to non-delinquent runaways?


Applicable Compact Provisions and Rules:

ICJ Article I

ICJ Article I in relevant part states:

“The compacting states also recognize that Congress, by enacting the Crime Control Act, 4 U.S.C. §112 has authorized and encouraged compacts for cooperative efforts and mutual assistance in the prevention of crime.”

“It is the purpose of this compact, through means of joint and cooperative action among the compact states to: (A) ensure that the adjudicated juveniles and status offenders subject to this compact are provided adequate supervision and services in the receiving state as ordered by the adjudicating judge or parole authority in the sending state; (B) ensure that the public safety interests of the citizens, including the victims of juvenile offenders, in both the sending and receiving states are adequately protected; (C) return juveniles who have run away, absconded or escaped from supervision or control or have been accused of an offense to the state requesting their return . . . (J) establish a system of uniform data collection on information pertaining to

	Interstate Commission for Juveniles	Opinion Number: 01-2014	Page Number: 2
<p align="center">ICJ Advisory Opinion Issued by: Executive Director: Ashley H. Lippert Chief Legal Counsel: Richard L. Masters</p>			
Description: The Health Insurance Portability and Accountability Act (HIPAA) as it relates to youth and family information.	Dated: January 23, 2014		

juveniles subject to this compact that allows access by authorized juvenile justice and criminal justice officials, and regular reporting of Compact activities to heads of state executive, judicial, and legislative branches and criminal justice administrators . . .”

ICJ Article III

ICJ Article III, K. provides as follows:

“The Interstate Commission shall collect standardized data concerning the interstate movement of juveniles as directed through its rules which shall specify the data to be collected, the means of collection and data exchange reporting requirements. Such methods of data collection, exchange and reporting shall, insofar as is reasonably possible, conform to up-to-date technology and coordinate its information functions with the appropriate repository of records.”


ICJ RULE 2-102: Data Collection

ICJ Rule 2-102-1 states as follows:

1. As required by Article III (K) of the compact, member states shall gather, maintain and report data regarding the interstate movement of juveniles who are supervised under this compact and the return of juveniles who have absconded, escaped or fled to avoid prosecution or run away. Each member state shall report annually by July 31st.

Analysis and Conclusions:

The first question posed by Rhode Island, as with any question regarding the application of HIPAA, should be analyzed in the context of the purpose of these privacy rules which were intended to protect an individual’s privacy while allowing important law enforcement functions to continue. (See **HIPAA Privacy Rule & Public Health, Guidance from Center for Disease Control and The U.S. Department of Health and Human Services, April 11, 2003**). Thus, HIPAA exempts certain disclosures of health information for law enforcement purposes without an individual’s written authorization. The various conditions and requirements concerning these exempt disclosures are contained in the regulatory text of the HIPAA privacy rule and may be found at **45 CFR 164 et. seq.** Under these provisions, protected health information may be disclosed for law enforcement purposes when a law requires such disclosures.

 Interstate Commission for Juveniles	Opinion Number: 01-2014	Page Number: 3
<p style="text-align: center;">ICJ Advisory Opinion Issued by: Executive Director: Ashley H. Lippert Chief Legal Counsel: Richard L. Masters</p>		
Description: The Health Insurance Portability and Accountability Act (HIPAA) as it relates to youth and family information.	Dated: January 23, 2014	

Based on these provisions and the above referenced provisions of the ICJ compact statute, clearly evincing an intent for the enforcement of laws concerning juvenile offenders and the protection of public safety, we have previously concluded in ICJ Advisory Opinion 1-2012 that disclosure of protected health information required to be furnished by or received from state agencies which administer the ICJ acting pursuant to the provisions of the compact and its authorized rules is permissible. [See **45 CFR 164.512 (f)(1)(i)**].


In addition, exempt disclosures include those in which a response is required to comply with a court order. [See **45 CFR 164.512 (f)(1)(ii)(A)-(B)**]. Based upon this exemption and the above reference provisions of ICJ Article I, it is equally clear that a principal purpose of the compact is to “*ensure that the adjudicated juveniles and status offenders subject to this compact are provided adequate supervision and services in the receiving state as ordered by the adjudicating judge or parole authority.*” Thus, as previously stated in ICJ Advisory Opinion 1-2012:

“Under this provision, the disclosure and tracking of protected health information, among authorized compact administrators’ offices, concerning any juvenile subject to compact supervision pursuant to court order, as required by the ICJ and its authorized rules would be exempt from HIPAA.”

Both the foregoing provisions of the compact and the ICJ rules require the compact member states to implement the law enforcement and public protection aspects of the compact through “a system of uniform data collection” (See Article I, J). It further specifies the means by which this purpose shall be achieved; “[S]uch methods of data collection, exchange and reporting shall insofar as is reasonably possible conform to up-to-date technology and coordinate its information functions with the appropriate repository of records,” (See Article III, K).

To comply with the mandates of the ICJ statute and duly authorized rules, the Commission developed the Juvenile Interstate Data System (JIDS), as identified above. This satisfies the HIPAA exemptions with respect to both Personal Identifiable Information (PII) as well as Personal Health Information (PHI).

With respect to the second question, regarding protection of the confidentiality concerning emails, the same analysis is applicable and the HIPAA exemptions cited herein can be applied to the law enforcement activity of the compact and states under the provisions of the ICJ statute and duly authorized rules. Moreover, the JIDS ‘application’, as set forth in JIDS Security documentation, “. . . is an electronic workflow system that facilitates state-to-state transfers, returns and travel for juveniles.” Access to the system is required through a “secure web portal

 Interstate Commission for Juveniles	Opinion Number: 01-2014	Page Number: 4
<p style="text-align: center;">ICJ Advisory Opinion Issued by: Executive Director: Ashley H. Lippert Chief Legal Counsel: Richard L. Masters</p>		
Description: The Health Insurance Portability and Accountability Act (HIPAA) as it relates to youth and family information.	Dated: January 23, 2014	

provides automation to paper-based processes and creates accountability through all steps in the process. InStream maintains Advanced Encryption Standards defined by the National Institute of Standards and Technology (NIST) for content storage and transmission.” (See JIDS Security Newsletter, attached and incorporated by reference herein). Further, the JIDS system meets the criteria set forth by NLETS, the interstate justice and public safety network for the exchange of law enforcement, criminal justice, and public safety related information and is furnished through a web service which is utilized by the U.S. Department of the Treasury and the U.S. Department of State, among others which require secure data exchange. Additionally, all information contained in JIDS is encrypted.


Finally, with regard to the application of the above referenced compact provisions and rules to non-delinquent runaways, reference is made to the more general provisions of the HIPAA privacy rules which allow disclosures of protected health information when consistent with applicable law and ethical standards, *including disclosures to a law enforcement official reasonably able to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public. [45 CFR 164.512 (j)(1)(i)]; or to identify or apprehend an individual who appears to have escaped from lawful custody [See 45 CFR 164.512 (j)(1)(ii)(B)].* (emphasis added).

As discussed in ICJ Advisory Opinion 1-2012, these provisions would apply to the return of juveniles who have absconded, escaped, fled to avoid prosecution or run away. Additionally, HIPAA specifically authorizes disclosures of protected health information to law enforcement officials who need the information in order to provide health care to the individual and for the health and safety of the individual. **[45 CFR 164.512 (k)(5)]**. Under these provisions, it appears that disclosures of health information required to provide treatment of juveniles subject to the ICJ, including non-delinquent runaways, would also be exempt from HIPAA requirements.

It is also important for compact administrators to be aware that at least one federal court opinion on the subject suggests that immunity from a private cause of action by an individual under HIPAA would apply to jurisdictions that are signatories to the interstate compact agreement in question. See Johnson v. Quander, 370 F.Supp.2d 79 (D.D.C. 2005).

Summary:

In sum, since the Commission, in compliance with the mandates of the ICJ statute and duly authorized rules, developed the Juvenile Interstate Data System (JIDS), as identified above, it

 Interstate Commission for Juveniles	Opinion Number: 01-2014	Page Number: 5
<p align="center">ICJ Advisory Opinion Issued by: Executive Director: Ashley H. Lippert Chief Legal Counsel: Richard L. Masters</p>		
Description: The Health Insurance Portability and Accountability Act (HIPAA) as it relates to youth and family information.	Dated: January 23, 2014	

satisfies the HIPAA exemptions with respect to both Personal Identifiable Information (PII) as well as Personal Health Information (PHI).

HIPAA privacy rules allow disclosures of protected health information when consistent with applicable law and ethical standards, including disclosures to a law enforcement official reasonably able to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public, or to identify or apprehend an individual who appears to have escaped from lawful custody.

Under these provisions, it appears that disclosures of health information required to provide for treatment of juveniles subject to the ICJ, including non-delinquent runaways, would also be exempt from HIPAA requirements.

JIDS Security Newsletter

Sent May 1, 2012

In preparation for the implementation of the Juvenile Interstate Data System (JIDS), the Technology Committee is publishing a number of short articles as part of the preparation process. Each article will discuss an aspect of the implementation with the goal of helping your staff to be prepared for a new way of doing business.

Overview of JIDS Security

JIDS is a web-based application developed for the Interstate Commission for Juveniles by InStream, Inc. The equipment to host JIDS is provided by Amazon on their government cloud servers.

The JIDS application is an electronic workflow system that facilitates state-to-state transfers, returns and travel for juveniles. The application's secure web portal provides automation to paper-based processes and creates accountability through all steps in the process. InStream maintains Advanced Encryption Standards defined by the National Institute of Standards and Technology (NIST) for content storage and transmission.

Site Security

InStream

Building security requires key card access at multiple points of entry into the building, into server areas, and document conversion work areas 24/7. Visitors are required to sign in when entering the InStream offices and are accompanied at all times.

The facility has security patrols during all non-business hours and is equipped with alarm monitoring and cameras at point of entry. Random audits occur on security logs, e-mail transmissions, system security and physical security.

Amazon Web Service

Amazon Web Service (AWS) datacenters are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass a two-factor authentication a minimum of two times to access datacenter floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

AWS only provides datacenter access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to datacenters by AWS employees is logged and audited routinely.

In order to provide end-to-end security and end-to-end privacy, AWS builds services in accordance with security best practices, provides appropriate security features in those services,

and documents how to use those features. AWS's compliance framework covers FISMA, PCI DSS, ISO 27001, SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70 Type II), and HIPAA.

Amazon's Federal Government Customers include:

- Recovery Accountability and Transparency Board
- U.S. Department of the Treasury
- National Renewable Energy Laboratory at the U.S. Department of Energy
- U.S. Department of State
- U.S. Department of Agriculture
- NASA Jet Propulsion Laboratory
- European Space Agency

Amazon Web Service meets the following criteria set forth by NLETS, the interstate justice and public safety network for the exchange of law enforcement, criminal justice, and public safety related information:

- Provides a secure environment with redundant technical infrastructure and onsite expertise monitoring hardware and connectivity 24/7/365
- Monitored by both fixed and pan-tilt/zoom security cameras
- Protected by intrusion detection system with panic button activation
- Two-factor authentication for building access
- Biometric authorization for data center access
- Extensive pre-employment background investigation process for employees with data access
- On-site building security and data center monitoring staffed 24/7/365
- Robust, scalable, private, secure network
- Back-up generator and uninterrupted power supplies to ensure no loss of power
- Network racks are equipped with temperature and humidity sensors that are centrally monitored
- Site is protected by sophisticated, dual fire suppression systems
- Secondary hosting services are located at a Disaster Recovery location, allowing for multiple business continuity plans
- Remote services provided 24/7/365 by on-site technicians

Application Security

JIDS is a web-based application developed by InStream, Inc. and hosted by Amazon Web Service for ICJ. InStream is responsible for implementation and maintenance of all technical security controls protecting the application, as well as administrative controls dealing with the development and support of the application. ICJ is responsible for the administrative controls related to the operation of the application.

Encryption

All information contained in JIDS is encrypted. Security features include:

- Encryption for documents 'at rest' and document storage

- IIS SSL compatible (a secure infrastructure based on public-key cryptography by using digital certificates with Secure Sockets Layer (SSL))
- Allows changing Anonymous & IUSR IIS accounts
- File permissions securable by NTFS and security groups
- Able to encrypt plain-text passwords
- 128 bit encryption

Authentication

Users are uniquely identified to the system by their email address authenticated with a password.

Password Requirements

Passwords shall:

- be a minimum length of eight (8) characters, a mix of lowercase, uppercase and one special character
- not be a dictionary word or proper name
- not be the same as the User ID
- be changed within a maximum of every 90 days
- not be identical to the previous ten (10) passwords
- not be transmitted in the clear outside the secure location
- not be displayed when entered

A user will be allowed five (5) login attempts before being locked out.

Password Recovery

Users have the ability to reset their passwords by requesting a recovery that will facilitate the user being able to reset their password.

Authorization

All data is properly secured with specific rights customized to a group, project or user based on their role. JIDS uses a role based access control model to ensure that individual user access rights are sufficient to perform their required job functions. The workflow set up in JIDS requires review and sign-off at several levels to ensure processes are reviewed and approved as they progress through the system.