Payer Question:

The production file extracts we send to Maine through HSRI will no longer have field level encryption as previously accepted and required by Onpoint. HRSI requires the files to be encrypted with the use of 7 Zip AES256 Bit encryption software and passwords on each side.

This addresses security and privacy while the files are in transit from WellPoint to HSRI but HSRI will be able to view PHI information such as SSN/contract number, etc. when they use the password and open the file.

How is HIPAA Privacy addressed in this situation? The vendor contracts with Maine but not WellPoint, so WellPoint does not have a business associate agreement with the vendor. A business associate agreement would cover such scenarios. How does Maine ensure the privacy of WellPoint members according to current HIPAA rulings to allow WellPoint to send over PHI to HSRI for viewing?

MHDO Response:

Licensed Insurance Carriers and Third Party Administrators are required under Maine law to submit claims data to the Maine Health Data Organization. In order to ensure the security of personally identifiable information and personal health information that is submitted to the MHDO Data Warehouse the MHDO is requiring data submitters to encrypt all files before uploading to the warehouse. This file-level encryption will ensure the confidentiality of all data, not just individual fields.

The Maine Health Data Organization is not a covered entity under HIPAA. It is Maine law that governs the collection, release and confidentiality of claims data. The MHDO's vendor is an extension of the Agency and is providing a service on behalf of the MHDO. As such a business associate agreement would not be applicable.

IT & Systems Security Protection

All MHDO Data Warehouse systems reside within NORC's secure facilities. These facilities have strictly controlled physical access and maintain boundary protection utilizing network firewalls, Intrusion Prevention System (IPS) and security monitoring using a unified situational platform. The IT environment is thoroughly documented and is managed through proven NIST 800-53 Rev.3 framework. Security provisions are established and maintained to include:

- Managed firewall and IPS
- Configuration management baselines: FDCC\USGCB for laptops, Center for Internet Security (CIS) benchmarks for network and server systems
- Least privilege access to system boundary

- Continuous physical and system security monitoring
- Managed security policies using domain group policies for complex passwords and mandatory renewal
- Domain-managed virus protection
- Access control procedures for data and systems
- Virus and spam filtering of email
- Encryption, FIPS 140-2 Level 2 – laptops (Full Disk), VPN connection (2-factor authentication), Encrypted backups tapes

Within the Data Enclave environment which houses MHDO systems users are logically separated within their work area and unable to remove any information without prior authorization from MHDO. Any inbound or outbound files are managed and audited by the NORC Data Custodians.

Annual security tests are conducted by a third party IT security auditor. This auditor conducts a design-level review of controls that support the security of the Enclave using NIST Special Publications 800-53 (Moderate-Impact assets) as the security standard, and an analysis of risks to electronic protected health information (ePHI) in the Enclave as a result of identified gaps. The auditor evaluated the design and implementation of the following aspects of the NORC System Security Plan (SSP) through:

- Stating roles and responsibilities for ownership and stewardship of the SSP,
- Stating the risk assessment, methodologies, processes and documents,
- The certification and authorization of acquired and developed systems,
- Operational controls, including contingency and incident response plans and maintenance plans,
- Considerations of personnel management and facilities and physical security management,
- The integrity of information and the integrity of communications (network) systems,
- The control of access controls, including authentication of access accounts and the approved movement of data to zones of varying degrees of security,
- The appropriate selection of controls from the NIST 800-53 catalog of controls (as a result of FIPS 199 classification and the Risk Assessment), and
- The policies and process documentation (standards, procedures, guidelines and audit records, where applicable) for the selected controls from NIST 800-53.

In addition, these annual security tests include penetration testing and simulated denial-of-service attacks. The NORC Data Enclave was recently awarded a federal Authorization to Operate by USDA's Economic Research Service.

The NORC Data Enclave complies with the following federal compliance guidance:

- NIST Special Publication (SP) 800-55, Security Metrics Guide for Information Technology Systems

- NIST SP 800-53, Recommended Security Controls for Federal Information Systems
- NIST SP 800-51, Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme
- NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems
- NIST SP 800-34, Contingency Planning Guide for Information Technology Systems
- NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems
- NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS 191, Guideline for the Analysis of Local Area Network Security
- IEEE Std 829-1998, IEEE Standard for Software Test Documentation

The NORC Data Enclave IT Security Plan is fully compliant with the Federal Information Security Management Act, provisions of mandatory Federal Information Processing Standards (FIPS), and meets all of NIST's IT, data, system and physical security requirements.

In addition to internal NORC confidentiality and ethics statements, all NORC Data Enclave employees must sign project specific Nondisclosure Agreements as specified in Commerce Acquisition Regulation (CAR) 1352.209-72, Restrictions against Disclosures.

NORC is in compliance with DOC IT Security Program Policy, section 4.5 and the NIST IT Security Management Handbook, including section 8.3 regarding policy on rules of behavior. The NIST Policy on IT Resources Access and Use must be followed for rules of behavior for this system.

The NORC Data Enclave is subject to the DoC IT Security Program Policy and Minimum Implementation Standards along with the IT security laws and federal regulations including:

- Public Law 107-347 E-Government Act of 2002 (FISMA included), Title V: Confidentiality Information Protection and Statistical Efficiency Act (CIPSEA).
- Public Law 200-253 Computer Security Act of 1987
- OMB Circular No. A-130 , Appendix III, Security of Automated Information Resources
- Department of Commerce Administrative Orders and
- NIST Administrative Manual Chapter 11.02 and the NIST IT Security

All NORC employees are explicitly trained to uphold respondent confidentiality. NORC employees must sign a legally binding pledge regarding this responsibility as a term of their

employment. In addition, members of the Data Enclave management team and task leaders must successfully complete the Human Participant Protections Education for Research Teams online training course sponsored by the National Cancer Institute, as well as CIPSEA and HIPAA certification.

I hope this information addresses the issues you raised. Please contact me with any additional questions. Thanks, Karynlee