ACF **Administration for Children and Families**	**U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES** **Administration for Children and Families**	
	1. Log No: ACYF-CB-IM-15-04	**2. Issuance Date:** July 1, 2015
	3. Originating Office: Children's Bureau	
	4. Key Words: Data breaches, Personally Identifiable Information, Confidentiality, Privacy, Cyber Security/State and Tribal Automated Child Welfare Information Systems (S/TACWIS), state or tribal automated child welfare information systems funded by Title IV-E	

INFORMATION MEMORANDUM

TO: State and Tribal Title IV-E Agencies; State and Tribal Information Technology Leadership; State and Tribal Data Security Leadership; and Other Interested Parties

SUBJECT: State and Tribal Child Welfare Information Systems, Information Security Data Breach Response Plans

LEGAL AND RELATED REFERENCES: 45 CFR 205.50 (a)(2)(i)(B); Section 471 (a)(8) Social Security Act

PURPOSE: This Information Memorandum (IM) provides a summary of key management practices state and tribal title IV-E agencies (agencies) may consider when developing plans to detect or respond to data breaches involving personally identifiable information (PII), personal health information (PHI), or confidential child welfare data. PII includes any information that can be used to distinguish or trace an individual's identity, such as name, date, and place of birth, social security number, or other types of personal information that can be linked to an individual, such as medical, educational, or financial information. PHI includes diagnosis, treatment, and prescription information. Confidential child welfare data includes but is not limited to abuse and neglect reports and investigations, removal, placement and adoption information.

States, tribes and local agencies are responsible for the security of information contained within child welfare information systems and should proactively mitigate risks associated with the inadvertent loss or unapproved disclosure of confidential information. As state and tribal child welfare information systems mature and government agencies continue to face significant security threats, the need to review and implement comprehensive data security programs is paramount. Agencies are encouraged to formalize data breach response plans to continually monitor and assess protocols, confidentiality requirements, system vulnerabilities and risk mitigation strategies. Key practice, risk mitigation and response strategies are summarized to strengthen agency security programs and local implementation efforts.

BACKGROUND: The number of reported information security incidents involving PII has more than doubled over the last several years, according to a 2014 US Government

Accountability Office report. A data breach is a security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Verbal, non-verbal, or written dissemination of confidential client data by a staff member may also be considered a data breach. The unauthorized access of a child welfare system, inappropriate sharing of sensitive information in conversation, posting or disclosing confidential information to a public website, sending protected information to incorrect recipients, misplacing information technology (IT) assets such as laptop computers or mobile devices or careless disposal of documents or IT resources may all lead to compromised information with harmful and costly results.

INFORMATION SECURITY PROGRAMS AND GUIDELINES FOR RESPONDING TO DATA BREACHES

Guidelines and standards for implementing information security programs are published by the **International Organization for Standardization (ISO)**, Federal Information Security Management Act (FISMA), Federal Information Processing Standards (FIPS), and National Institute of Standards and Technology (NIST) to assist organizations in developing and improving agency security. The Office of Management and Budget (OMB) Memorandum **M-07-16,** *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* outlines multiple security standards for easy reference. While each agency and system is unique, general guidelines for developing and implementing data breach response plans are summarized below:

PHASE I: PREPARATION BEFORE THE BREACH:

- ***Review your system and identify where sensitive information resides:*** Possessing data awareness means having a complete view of enterprise data sources. Agencies should develop an enterprise data map noting confidential PHI, and PII data. System reviews should include analysis of unstructured areas such as email, loose files on local drives and networks, hard copy documents as well as data exchanges and transfers for data coming into and out of the organization. Data source reviews should also include replicated environments, backup storage, archived and encrypted data, and data stored on or generated by mobile devices. Agencies are encouraged to conduct regular risk assessments and evaluate privacy threats for the organization, as well as any contractors, vendors, and other business partners. It is important to review access restriction practices and user activity so that accounts are current or deactivated appropriately.

- ***Assess applicable confidentiality and breach notification laws:*** A part of the preparation for an effective breach response involves assessing applicable confidentiality or privacy laws and evaluating your organization's legal responsibilities to notify affected parties. Depending upon the systems or compromised data, there may be legal notification requirements for data owners and other stakeholders. Most states have some form of data breach notification laws. Federal laws, including, the Gramm-Leach-Bliley Act, the Federal Trade Commission Act, the Health Information Technology for Economic and Clinical Health (HITECH) Act, and Federal Educational Rights and Privacy Act (FERPA), all address the importance of protecting sensitive information and

may potentially apply to agency information in the event of a breach. These laws vary in their requirements regarding the right of the individual to be notified of any potential loss or access to their sensitive information.

- ***Assess organizational risks and threats:*** Given the high volume of sensitive information handled by child welfare staff daily, it is easy for staff to become desensitized to potential data breach threats. Agency mitigation efforts should include reviews of technical and business opportunities for confidential information to be sent to or shared with the wrong recipient. Child neglect and abuse disposition letters, case plan or treatment information, visitation logs, safety assessments, social histories, adoption home studies and many other routine child welfare documents may be at risk if an agency's master client index or address information is not kept current or is modified during system enhancement initiatives. Likewise, hard copy documents or information stored on flash drives may be at risk if they are not incorporated into an agency's ongoing risk mitigation efforts.

  Each child welfare agency is different and faces a unique blend of requirements and threats, which make a single prescription for data breach response impossible and undesirable. Agencies are encouraged to conduct their own risk assessment to identify potential threats to their data systems and to sensitive information. The severity of different kinds of breaches should guide mitigation and response strategies. For a more in-depth discussion and a list of specific elements within each data breach plan component, see section 2.3, NIST special publication 800-61 rev.2.

- ***Develop organizational policy:*** Each child welfare organization should create a data breach response policy, approved by the organization's leadership and germane to its environment. The purpose of the policy is to establish goals and vision for the breach response process. Policy should have a clearly defined scope. The scope should state to whom the policy applies and under what circumstances. Policy should include:

  - the definition of a breach,
  - staff roles and responsibilities,
  - standards and metrics that can enable prioritization of the incidents, and
  - reporting, remediation, and feedback mechanisms.

  The policy should be well publicized and easily available to all personnel whose duties involve data privacy and security protection. Agencies are encouraged to establish employee expectations in conjunction with Human Resources (HR) policy and employee agreements.

- ***Develop a Data Breach Response Plan:*** A data breach response plan is a high-level strategy for implementing the data breach policy. Individual elements of the plan should cover all phases of the incident response, from reporting the breach and the initial response activities to strategies for notification of affected parties, including a breach response review and remediation process. The plan should identify the necessary organizational resources and required management support, such as senior management approval. It is important that the plan is highly tailored to your organization's unique

context and is in alignment with your organization's overall mission and goals. Typical integrated response teams for a child welfare system might include a senior manager team lead (with an identified back up) and representatives from IT and security offices, child welfare program and policy, communications, legal, contract and budget personnel. Agencies are encouraged to conduct regular reviews of the plan to incorporate improvements and updates as employees retire or transition to other jobs.

Special Considerations for Data Breach Plans:

- Include examples of types of breaches, applicable laws, stakeholders and harm impact from potential release.
- Develop guidelines for when you will use in-house resources or outside service providers to assist with investigation and mitigation efforts.
- Seek advice from legal and IT forensic auditors on approved methods for protecting digital evidence so it can be used in a court of law if necessary.
- Consider alternatives to replace or clear compromised resources; include cost of remediation or rebuilding assets.
- Identify communication point of contact and know when law enforcement, legal counsel, chief inspector, auditor or others should be consulted.
- Develop guidelines and templates for notifying affected parties and stakeholders via internal communication, mail, email, or telephone.
- Develop media notification guidelines, and when possible, notify affected individuals **prior to media releases**.
- Provide data security guidelines to assist staff with compliance.
- Document mitigation resources and alternatives, such as credit monitoring or identity theft protection services.

- ***Develop program procedures and practice:*** Procedures are derived from the breach response plan and codify specific tasks, actions, and activities that are a part of the data breach response effort. Procedures are designed to standardize behavior so that response activities are handled in an efficient, documented, and repeatable way, while minimizing the introduction of errors. Breach response procedures should be periodically reviewed, practiced and tested in conjunction with other business continuity and disaster recovery procedures to test their effectiveness and identify improvement priorities.

- ***Train employees:*** Agencies should train employees, users and contractors on data breach policies and response plans. It is critical that staff understand their responsibilities both in terms of protecting confidential data and in responding effectively when a breach occurs. Security and confidentiality training should be provided to end users prior to system access and refresher training should be provided periodically.

- ***Implement security controls and monitor continuously:*** Agencies should implement mitigation and security controls, such as prevention and detection tools, mobile device management systems and encryption standards to minimize risk of data breaches and continuously monitor for sensitive data leakage and loss. Automated tools, like detection or prevention systems, application performance management systems, next generation

firewalls, and anti-virus and anti-malware tools to monitor and alert suspicious activity are likely already deployed in most organizations. It is also important to regularly search your system to identify PII, PHI, or confidential child welfare data that may be stored outside of approved areas. Some agencies conduct periodic internet searches to locate protected information that is available in the public domain or visible to the public. Periodic testing of security controls through real life exercises may also be helpful to assess the effectiveness of risk management programs.

- ***Define and post privacy policies and make incident reporting easy for stakeholders*:** Agencies are encouraged to post and communicate privacy policies to customers, staff and users via communications channels such as the agency web page or on bulletin boards, and should implement an accessible process for reporting privacy incidents and complaints.

PHASE II: RESPONDING TO THE BREACH:

- ***Validate the breach*:** Do not assume every identified incident is actually a breach of PII, PHI, or confidential child welfare data. Examine the initial information and available logs to confirm that a breach has occurred. If possible, identify the type of information disclosed and estimate the method of disclosure, whether internal or external disclosure, malicious attack, or accidental release of information. It is important to ensure validation activities do not compromise files or evidence that may be needed later in the investigatory process.

- ***Assign a senior level manager to coordinate an incident response team and coordinate between multiple organizational units*:** Begin breach response documentation and reporting process. Coordinate the flow of information and manage public message about the breach.

- ***Assemble incident response team*:** Engage appropriate parties from management, child welfare, IT, legal, public affairs or media relations, risk management, finance and audit departments, and if appropriate, representation from such units as HR, Auditor and Inspector General's office.

- ***Assess status of the breach*:** If active or ongoing, take action to prevent further data loss by securing and blocking unauthorized access. Document all mitigation efforts for future analysis. Advise staff members to keep details in confidence until notified otherwise.

- ***Determine scope and composition of breach*:** Assess criminal activity and notification requirements. Identify all affected data, machines, and devices. Conduct interviews and document facts.

- ***Preserve evidence (back-ups, images, hardware)*:** Locate, obtain and preserve all written and electronic logs and records applicable to the breach when possible.

- ***Follow Communication Protocol and reach out to and notify data owners:*** Work collaboratively with data owners to secure sensitive data, mitigate damage and determine root causes. Follow communication protocols and internal and external notification timelines.

PHASE III: POST BREACH INCIDENT ACTIVITY:

- ***Systematically document suspected data breaches***: Agencies should consistently document and review suspected data breaches regularly.

- ***Determine probable cause and minimize risk of future occurrence***: Data breach documentation should include an analysis of probable cause, as well as mitigation strategies, to reduce the likelihood of future occurrence.

- ***Address and mitigate cause***: Mitigation strategies should be based upon actual incidents and regularly assessed for efficacy.

- ***Solicit feedback from responders***: Agencies are encouraged to solicit feedback from response team members in reporting breaches and assessing risk mitigation effectiveness.

- ***Review breach response, send feedback and analyze trends:*** Document information for understanding trends (time taken to respond or notify, cost of investigation and mitigation efforts, types of breach, and types of violation or threats).

- ***Analyze and document lessons learned***: Each data breach response practice exercise, audit and incident provides important opportunities for agencies to improve information systems and incident responses. As organizations face an unprecedented number of internal and external security threats, encouraging a learning approach to managing data security is critical.

- ***Modify breach response plan, strategies and security controls***: Effective data breach response plans are living documents incorporating agency specific knowledge and accumulated history of incidents and mitigation strategies. Agencies should continually assess the effectiveness of prevention/detection tools to ensure proactive risk management resources are optimized.

- ***Enhance and modify information security and training programs***: Most agencies have data security and training programs. Additional data breach planning resources are referenced at the end of this Program Instruction.

- ***Offer assistance to affected individuals, if appropriate***: Aside from providing notification, credit monitoring and sharing mitigation responses are typical ways organizations respond to affected individuals. Based upon the unique circumstances and laws applicable to the breach, other assistance may be appropriate.

INQUIRIES: Director, Division of State Systems, CB/ACYF/ACF/DHHS

/s/

Mark Greenberg
Acting Commissioner,
Administration on Children, Youth and Families

/s/

JooYeun Chang
Associate Commissioner
Children's Bureau

Attachment

FURTHER READING:

Legislation, Rule, and Regulation:

- Child Abuse Prevention and Treatment Act (CAPTA) 106 (b) (2) (B) and 106 (c) (5) (A): https://www.acf.hhs.gov/sites/default/files/cb/capta2010.pdf
- HIPAA Breach Notification Rule, 45 CFR 164.400-414 http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html;
- Health Information Technology for Economic and Clinical Health (HITECH) Act section 13407: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf
- Congressional Research Service, Federal Information Security and Data Breach Notification laws (January, 28, 2010); RL34120: www.fas.org/sgp/crs/secrecy/RL34120.pdf

National Conference of State Legislatures:

- Security Breach Notification Laws: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Federal Government Resources:

Federal Trade Commission:

- Dealing With A Data Breach: www.ftc.gov/bcp/edu/microsites/idtheft/business/data-breach.html
- Complying with FTC's Health Breach Notification Rule: http://business.ftc.gov/documents/bus56-complying-ftcs-health-breach-notification-rule
- Data Security: http://business.ftc.gov/privacy-and-security/data-security
- Information Compromise and Risk Identity Theft: Guidance for Your Business: http://business.ftc.gov/documents/bus59-information-compromise-and-risk-id-theft-guidance-your-business
- Mobile App Developers: Start with Security: http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security
- Protecting Personal Information: A Guide for Business: http://www.business.ftc.gov/documents/bus69-protecting-personal-information-guide-business

United States Department of Education:

- Privacy Technical Assistance Center: Data Breach Response Checklist: http://ptac.ed.gov/sites/default/files/checklist_data_breach_response_092012.pdf

Office of Management and Budget:

- Memorandum: *Recommendations for Identity Theft Related Data Breach Notification*: http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/task_force_theft_memo.pdf

United States Department of Health and Humans Services:

- Personally Identifiable Information (PII) Breach Response Team (BRT) Policy: http://www.hhs.gov/ocio/policy/20080001.003.html
- Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response http://www.hhs.gov/ocio/policy/hhs_ocio_policy_2010_0004.html

Multi-Agency Task Force Resources:

- Internet Crime Complaint Center (IC3): http://www.ic3.gov/default.aspx