Testing Experience and Functional Tools Demonstration: Personal Health Record (PHR) User Survey

Paperwork Reduction Act Submission

Appendix B: Personal Health Record Survey Instrument Data Security Plan

CMS-10623
OMB Control Number: 0938-New

Personal Health Record User Survey Instrument

Purpose: The purpose of this document is to describe the data security measures and procedures to protect the Personal Health Record (PHR) user survey data. Our data do not contain personally identifiable information (PII) or protected health information (PHI).

Project Description: The goal of the Testing Experience and Functional Tools (TEFT) Demonstration is to advance the development and use of standardized quality metrics for community-based long-term services and supports (CB-LTSS) and adoption of an e-LTSS standard, linked to a PHR and fully integrated into states' overall quality improvement and information technology strategies. One component of TEFT is developing, testing, and piloting a PHR among Medicaid CB-LTSS beneficiaries in six states.

The Lewin Group (Lewin) under a contract with Centers for Medicare & Medicaid Services (CMS) will receive, manage, and transfer data that a sample of Medicaid CB-LTSS submits anonymously through an online survey[1]. While the data will not contain PII or PHI, appropriate precautions will still be employed for accessing, transferring, and storing data. PHR survey data will not reside on a public facing server and will be handled according to Lewin's security policies. Lewin's full Data Management, Protection, and Security Plan is provided at the end of this document.

PHR Survey Data: Lewin will work with six TEFT states to disseminate the PHR User Survey to their Medicaid CB-LTSS populations that have been offered a PHR. The sample size for all six states is 720 beneficiaries. CMS and Lewin expect to receive responses back from 80% of the sampled population.

PHR Survey Data Flow: The data flow and associated security measures are outlined below.

1. Lewin will develop a unique survey link for each state participating in the PHR component of the TEFT Demonstration. Lewin will send this link to each state.
2. The state will be responsible for disseminating this link to their targeted Medicaid CB-LTSS users for the PHR component (referred to as "beneficiaries" moving forward). Lewin will not receive names or contact information of these beneficiaries. The state will not be able to link the survey responses back to any beneficiaries.
3. Beneficiaries will have the option to complete this survey. It is a completely voluntary survey. The survey does not ask for a name or other PII or PHI. Limited demographic information will be collected (e.g., age range, sex).
4. The beneficiary will submit the survey after completing it online. Data will be maintained on Research.net, which is appropriately protected with Secure Sockets Layer (SSL) and Transport Layer Security (TLS) technology and uses both server authentication and data encryption.
5. Lewin will export the data from Research.net and maintain the data on a password-protected folder and secured on a private network.
6. Lewin will analyze the data on an aggregate level for each state.
7. Lewin will provide a summary report to CMS.

Security Safeguards and Procedures: As described in the PRA ***Supporting Statement A*** for this survey, the methodology for the PHR User Survey is intended to ensure the anonymity of survey respondents. The TEFT evaluation team, CMS, and states will collaborate to ensure this data collection effort is implemented effectively and in alignment with federal and state policies and industry Internet security practices. The TEFT evaluation team will employ the following safeguards to carry out confidentiality assurances:

[1] Respondents will have the option to submit a paper-based survey upon request.

- Access to identities of potential respondents will be limited to the state staff
- Contact information and PHI will not be collected in survey responses
- Data analyses and reports will reflect aggregate findings, never on the individual respondent level
- Data when in transit from Research.net to the TEFT evaluator will be secure
- Access to survey data will be strictly limited to those who are responsible for entering and analyzing data
- A consent statement will be included, if requested by a state
- Sampled respondents are not required to participate and can opt to not respond to any question

Specifically, all data collection activities will safeguard respondent confidentiality and anonymity as per the guidelines of the Privacy Act. CMS also provides assurance that the data collected are exclusively for statistical purposes and individuals will not be identified in any analyses or reports. CMS is able to provide this assurance under the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA) (Pub. L. No. 107-347, title V). Specifically, the TEFT evaluation team will not solicit respondents' names, and will ask respondents to provide minimal demographic information (e.g., sex, education), allowing web-based survey responses to be submitted anonymously. The TEFT evaluation team will not attach any codes or addresses to responses. Further, respondents who request a paper-based survey will be asked to submit their completed documents in a return envelope that will not require participant identifiers, such as name and address. Finally, upon analysis of the survey responses, reports will not identify any individual respondents. No state agency will take any action to the benefit or detriment of responders or non-responders' program participation.

The TEFT evaluation team will not have access to any individual's contact information or PHI. The TEFT states will oversee communications to individuals in the survey samples. The TEFT evaluation team intends to use Research.net for online surveys and create a unique web address for each state's survey. The TEFT evaluation team will track the denominator and numerator of responses in each state, but will not track individual-level non-response or duplicate submissions. Reports presenting the survey findings will not identify any individual respondents. All personally identifiable information will be destroyed at the study's conclusion.

Security

The respondents' data when in transit from the survey website to the TEFT evaluation team will be safe, secure, and available only to TEFT evaluation staff assigned to the tasks of data collection and analysis. Communications with the Research.net website will be appropriately protected with Secure Sockets Layer (SSL) and Transport Layer Security (TLS) technology and using both server authentication and data encryption. Research.net maintains industry security protections related to user security, physical security, availability, network security, storage security, and organizational and administrative security.

The TEFT evaluation team's security protections once the survey data are transmitted from Research.net will include storage in a password-protected folder and secured on a private network. The TEFT evaluation team provides privacy and security training to the TEFT team staff annually. Additionally, access to the survey data files will be set on a need-to-know/least privilege necessary basis. The TEFT evaluation team also maintains information security policies, including incident response plans, and regularly reviews and updates them. For paper-based surveys, documents will be stored in locked files and cabinets and completed materials will be shredded.

Because the survey does not solicit PHI, the TEFT evaluation team and respondents will not require HIPAA-enabled accounts.

Consent

Prior to data collection, the TEFT evaluation team will discuss with state staff and strictly follow any state-level policies related to consent in state quality improvement/assurance initiatives. The TEFT evaluation team will address consent as specified by the needs of each state. If requested by the state, the TEFT evaluation team will add a consent acknowledgement in the online and paper-based surveys (if paper is requested). Research.net provides the capability to ask respondents to agree to a consent statement outlining data transfer practices, privacy practices or other policies. Research.net also includes "no response "or "prefer not to respond" as an option for questions. The TEFT evaluation team will include "prefer not to respond" to questions at the request of any TEFT states, as per state policies. Additionally, in the survey introduction, respondents will be informed that participation is voluntary and information provided will be confidential.

Lewin will not be using any subcontractors for this survey dissemination, data collection, and analysis.

Administrative Controls:

1. Assignment of Security Responsibility: The Lewin TEFT Project Manager is responsible for ensuring all Lewin employees, contractors, and consultants working on the project comply with the security measures described in this security plan.
2. Confidentiality Agreements: There are no required Business Associate Agreements, Data Use Agreements, and additional documentation required by state agencies.
3. Reporting of Security Breaches: All staff shall be aware of their duties to report breaches or suspicious activities as soon as possible after observation of the breach.
4. Security Training: Lewin requires that all employees understand and abide by data privacy, security, and confidentiality policies through a combination of agreements and required security training. All new Lewin employees must attend a privacy and security training course and repeat it annually.

The Lewin Group: Data Management, Protection and Security Plan

Information Systems and Security

Lewin has fully operational information systems to perform its information technology (IT) functions for the CMS TEFT Demonstration. Lewin has developed rules and procedures that all its employees and subcontractor employees must follow to maintain information security and privacy. Our system has security controls to protect the confidentiality, integrity, and availability of systems operations. We have specific standards in place to transmit, receive, manage, and store Federal information. Lewin has implemented policies and procedures based on best practices, risk assessment, and legislative and contractual requirements for privacy and security set by HHS-OCIO Policy for Information Systems Security and Privacy, the Centers for Medicare and Medicaid Services' information security policies, Federal Information Security Management Act of 2002 (FISMA), FedRAMP, other Federal and State laws, and other Federal agencies. The Lewin Security Officer, Ed Mounib, and Director of IT, Brad Harrison ensure policies are updated and reviewed annually.

Lewin has an IT Plan which includes an Information Security Risk Assessment (ISRA), Systems Security Plan (SSP), Security Controls, E-Authentication Workbook, Contingency Plan (CP), Contingency Planning Tabletop Test Plan, Contingency Planning Tabletop Test – After Action Report, and HHS Privacy Impact Assessments (PIA). As needed, we have Data Use Agreements with other entities.

Data Management

Access is granted to only the authorization level appropriate for each user (e.g., read-only, update, delete, print). Routine auditing of access and data security will be compared to authorized users listed in the data library.

Specific methods of data sharing and transfer as well as storage are discussed later in this section. Original media is stored in locked safe where access is limited and audited or it is destroyed. Identifiable or sensitive data is stored electronically on a secured server maintained in accordance of the CMS security controls. All network access is limited and requires multi-factor authentication. Raw data files are uploaded to servers via drive mapping using a secure VPN connection. Access, all connections, and file transfers are audited. Files are not be comingled.

System Description

Lewin's information technology infrastructure maintains a sophisticated gigabit switched local area network (LAN) equipped with multiple Windows servers and a network attached storage (NAS) device, utilizing snapshot technology and providing several terabytes of secure data storage. The LAN connects over two hundred personal and virtual computers. Over ninety percent of consultant computers are laptops. Each computer operates using Microsoft Windows operating system and is equipped with Microsoft Office Professional utilizing our secure document management system. Our servers maintain a high availability using

redundant components, RAID and hot swappable parts. Lewin maintains a sophisticated virus and spam protected clustered e-mail server farm using Microsoft Exchange that allows Lewin staff to exchange email and data files internally as well as externally via our redundant Internet connection. Lewin has Internet and World Wide Web connections that provide our staff with data communication capabilities by secure multi-factor authentication website for file transfer, network modems, and Internet to other electronic mail locations and networks, as necessary. Each computer facility maintains security measures to protect client confidentiality and corporate security.

Lewin utilizes a high-speed SAS server enabling staff to process remotely more than 8 terabytes of data at a time with additional 41 terabytes available in near-line storage. The Lewin Group system utilizes workstation assets on the Lewin LAN to initiate the job processes completed by the Lewin system. Lewin analysts utilize the LAN resources to conduct their day to day operational requirements; the Lewin LAN provides connectivity for Lewin system users to the high-speed SAS server. Lewin maintains and manages the infrastructure, operating system, storage, backups, database instance security, patching, and database instances for disaster recovery.

Security

Network resources on Lewin systems are secured and protected using three tier architecture, network access control (NAC), file level access control lists (ACL), network authentication via Active Directory, strong password management, and anti-virus/antimalware scanning. Computer security is maintained via localized firewalls, mandatory password-protected screen savers, FIPS 140-2 compliant hard-disk encryption and removable media protection. The network perimeter is secured and protected using an enterprise-level firewall, client virtual private network (VPN), enterprise-level anti-virus/anti-malware protection, two-form-factor authentication and intrusion detection systems (IDS). Data access is granted only by authorization of the of the data/project owner. The project manager approves and manages individual’s access to the data. Access audits are conducted annually. Requests and approvals are then documented in our enterprise helpdesk ticketing system as reference. Unauthorized access in not permitted without exclusive access rights being granted. Security updates and anti-virus definitions are automatically deployed to all nodes to minimize risk due to vulnerabilities. Lewin utilizes tapeless disk based backup solution with data securely replicated to Lewin’s disaster recovery site.

1. Personnel Security Controls

All Lewin employees have background checks before they are hired. Employees who are assigned a company computer are given unique password(s) which limit access on a need-to-know basis. Employees are instructed to log out of own computer if away from it for an extended period of time, not share any system password(s) and not post their password(s).

The logon screen warning banner notifies the user that the system processes confidential information and it is subject to monitoring each time they log on. The warning banner notifies users of acceptable use of the computer system and its resources, data, and network access capabilities. It includes notice of authorized monitoring of users' activities while they are using the system, and warnings of legal sanctions should the authorized monitoring reveal evidence of illegal activities or a violation of security policy.

Computer passwords must be at least 8 characters in length; include 3 of 4 character types, lower case alpha, upper case alpha, numeric with special characters; passwords are not displayed when entered; password minimum is 2 days, maximum is 60 days; passwords are prohibited from reuse for at least 10 generations; and passwords are changed when an individual changes positions. Password protected screensavers (e.g., the login screensaver or blank screen) are displayed after 15 minutes of inactivity. An account is suspended after three unsuccessful login attempts.

Any access to sensitive data must first be approved by the data/project owner before IT staff allows access. Requests and approvals are then documented in our enterprise helpdesk ticketing system as reference. Unauthorized access is not permitted without exclusive access rights granted.

Lewin, and its parent company Optum, require all employees regardless of job duties, job title or past experience to take the privacy and security training course "It's Personal- Privacy and Security". The course provides employees with a basic understanding of the importance of securing protected and confidential information and explains company policies, procedures, and practices for securing these data. Security training is held at least every 12 months and is in compliance with FISMA requirements.

Lewin currently has a Security Officer with responsibilities company-wide to ensure the privacy and security of protected health information and personally identifiable information. Lewin has established procedures for reporting confidentiality infractions and devotes resources to maintaining privacy and security awareness. Any security incidents are reported to the Security Officer. The Security Officer will clearly and accurately report any incident according to Lewin's Security Monitoring and Response Policy (Section 06.0) and our clients' requirements. The Security Officer will document the actions taken to correct the security incident and prevent recurrence.

2. Physical Security Controls

Lewin's office building has physical security systems in place to prevent unauthorized entry and access to both computer systems and hard copies of files. The office has a key pass entry system with a receptionist on duty during working hours. During non-working hours, the office is accessible to key holders only. Additionally the building is patrolled by a security officer throughout the day and remotely monitored by video cameras in the elevators and other building entrances.

Lewin maintains a universal System Contingency Plan which establishes procedures to recover all Lewin systems, following a service disruption. The following objectives have been established for this plan:

> Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
> ***Notification and Activation phase*** to detect and assess damage and to activate the plan
> ***Recovery and Restoration phase*** to restore temporary IT operations and recover damage done to the original system
> ***Return to Normal Operations phase*** to restore IT system processing capabilities to normal operations.
> Identify the activities, resources, and procedures needed to carry out the system's processing requirements during prolonged interruptions to normal operations.

Assign responsibilities to designated personnel and provide guidance for recovering the system during prolonged periods of interruption to normal operations.
Ensure coordination with other Lewin staff and system owners of interconnected systems who will participate in the contingency planning process.

Ensure coordination with external points of contact and providers as needed.

Optimally, the Lewin Contingency Plan contains enough detailed information to ensure that all business processes can be performed following the loss of all or most of the management experts as well as the loss of equipment and/or automated systems.

The network servers and attached storage are installed in a secured, Lewin-controlled server room. The secured server room has environmental controls, restricted access to non-authorized personnel, and dedicated power. The server room has advanced environmental controls that ensure proper heating and cooling of the system components. Authorized personnel must use a secured proximity card to enter and display proper identification at all times. In addition, all non-Lewin personnel must be escorted at all times. The exception is facility maintenance personnel who have been cleared by Lewin security and do not need escorts when Lewin personnel are not available. The server room also has an alarm system in place to ensure no unauthorized after-hours access is possible. The alarm system is monitored twenty-four hours a day, seven days a week and a response takes place when any alarm is triggered. All of the Lewin System servers are protected by an Uninterruptible Power Supply (UPS) in place to prevent improper shutdown of the systems due to the loss of power, the UPS provides sufficient power back up to ensure graceful shutdown.

3. Data Transfer and Storage

Data transfer of sensitive data to and from subcontractors, federal and state agencies, and other clients are completed via a multi-factor authentication secure website (MFA Website) supporting filesharing or through physical transfer of removable media, typically compact disks (CD). Lewin encrypts and password protects all datasets using SecureZip which meets FIPS 140.2 security standards. Any media that contains federal agency sensitive data is labeled “[Agency] Sensitive Information”. E-mail is used to transfer data only if the data contains no sensitive information. Sensitive information includes any type of personally identifiable information (PII), health information (PHI) or social security numbers (SSN). If sensitive information is mistakenly emailed and/or transferred, Lewin has an incident reporting protocol which is supervised by the Lewin security officer and includes destroying the sensitive information, informing the sender of their action and logging the incident.

Sensitive data files that are received by MFA website or on CDs are transferred to our secure SAS server to be processed. The secure SAS server is accessible only to a limited number of team members for the specific project. The CDs are locked in a metal security container, with access available only to authorized staff. Confidential hardcopy data is secured and kept out of sight from unauthorized persons. Disposal of sensitive hardcopy material is by shredding. Lewin maintains two locked shredding bins that are picked up monthly for secure off-site document destruction.

Fax procedures for sensitive information include several safeguards. The fax number is verified before transmittal. A trusted staff member attends both the sending and receiving fax machines. A cover sheet includes notification of sensitive data, need for protection and instructions to unintended recipients.

4. Internet Services

Lewin provides a wide range of Internet-based services including web hosting, list servers, MFA website access, SharePoint Team rooms and electronic mail. Lewin Internet Hosting services are firewall protected in a secure data center under 24 hour surveillance with redundant power and Internet access.

5. E-Mail

Lewin maintains a sophisticated virus and spam protected clustered e-mail server farm using Microsoft Exchange that allows Lewin staff to exchange e-mail and files internally as well as externally via our redundant Internet connection.

6. Review of Security Controls

All system maintenance and upkeep is performed by the Lewin Technical Assistance Center. A formal vulnerability test and a review of the security controls for moderate system sensitivity level are conducted annually using a Privacy Impact Assessment (PIA) under FISMA. The Blue Canopy, on behalf of the Centers for Medicare & Medicaid Services (CMS), conducted a Security Controls Assessment (SCA) of the Lewin system in June 2015 and again in October & November 2015. We have CMS approved Authorization to Operate (ATO). As part of the ATO, Lewin system controls are audited annually as part of the ATO. Lewin also maintains internal policy for Patch and Vulnerability Management Process which is updated on an annual basis.