Attachment 4a: Data security fact sheet

Form Approved
OMB Control # 0920-XXXX
Expiration Date: XX/XX/20XX

Collection of this information is authorized by The Public Health Service Act, Section 411 (42 USC 285a). Rights of study participants are protected by The Privacy Act of 1974. Participation is voluntary, and there are no penalties for not participating or withdrawing from the study at any time. Refusal to participate will not affect your benefits in any way. The information collected in this study will be kept private to the extent provided by law. Names and other identifiers will not appear in any report of the study. Information provided will be combined for all study participants and reported as summaries. You are being contacted to participate in this data collection so that we can further understand how psychosocial distress screening practices are implemented for lung and ovarian cancer survivors.
Public reporting burden for this collection of information is estimated to average 20 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. **An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number.** Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to: CDC/ATSDR Information Collection Review Office, 1600 Clifton Road NE, MS D-74, Atlanta, Georgia, 30329; ATTN: PRA (0920-XXXX). Do not return the completed form to this address.

Disparities in Distress Screening among Lung and Ovarian Cancer Survivors
Centers for Disease Control and Prevention (CDC)

Data Security Fact Sheet

This document presents information about data security for the CDC project entitled *Disparities in Distress Screening among Lung and Ovarian Cancer Survivors* project.
It explains:

- CDC project legal requirements regarding handling and storing of hospital EHR data, (including distress-screening data), and qualitative interview/focus group data
- Data security protocols and file transfer practices for this project

Legal Requirements

The Centers for Disease Control (CDC) project, Disparities in Distress Screening among Lung and Ovarian Cancer Survivors, abides to legal requirements for safeguarding electronic health information and qualitative data are governed by the following standards in the HIPAA Privacy Rule 45 CFR 164.514(e)(3)(ii) for limited datasets.

In addition, CDC complies with the Federal Cybersecurity Enhancement Act of 2015. This law requires the federal government to protect federal computer networks by using computer security programs to identify cybersecurity risks like hacking, internet attacks, and other security weaknesses. If any cybersecurity risk is detected, the information system may be reviewed for specific threats by computer network experts working for the government (or contractors or agents who have governmental authority to do so).

Each of these laws have been designed to protect the records of individuals; limit use; inform respondents; protect federal computer networks, and enable Westat as CDC's contractor to act as its Designated Agent.

CDC staff and its agents are required annually to complete training on confidentiality requirements and practices, including reporting any breach of confidentiality, and to sign annual non-disclosure agreements confirming intention to abide by all rules and regulations protecting confidential data. Contractor organizations are required to meet the same administrative, physical and technical safeguards as CDC and to agree in writing to the

same restrictions and obligations with respect to safeguarding confidential information collected in the *Disparities in Distress Screening among Lung and Ovarian Cancer Survivors* project.

Westat's Data Security Protocol

Westat, the contractor for the *CDC Disparities in Distress Screening among Lung and Ovarian Cancer Survivors* project uses guidelines established by the National Institute of Standards and Technology (NIST; 800-series) for meeting the requirements of the Federal Information Security Management Act (FISMA). Westat complies with all relevant laws, regulations, and policies governing the security of data and the protection of confidentiality.

From the Hospital to Westat – Secure Transfer

- Limited EHR and distress screening data will be transmitted from the facilities via Westat's Secure File Transfer System (SFTP) that provides a secure data transfer service that meets CDC policies for data transmission via the Internet. If the hospital agrees, Westat will access EHR data remotely using Westat's remote abstraction security requirements that meet FISMA, encryption, and FedRAMP requirements. The SFTP provides the secure data network and transmission mechanism needed to receive and store data files from participating hospitals. All files sent via the SFTP are securely stored and transferred using Federal Information Processing Standard (FIPS) 140-2 validated Advanced Encryption Standard (AES) encryption. Data are encrypted both during transmission and when stored on the Westat server. Login and password is required to access the SFTP server.

From Westat to CDC – Secure Transfer

After processing and coding of data, these data will be sent to the CDC via Westat's SFTP in the following summarized format:

- De-identified EHR patient data
- De-identified and coded data on distress screening and follow-up care
- De-identified transcripts and summary notes of individual interviews and focus groups