DUA Addendum

This amendment is made to the Data Use Agreement (#:) (DUA) by and between, the Centers for Medicare and Medicaid Services (CMS) and the Utah Department of Health and Human Services, hereinafter the "Department" dated [fill in].

It is mutually understood and agreed by and between the undersigned parties to amend the previously executed Agreement as follows:

1. Notwithstanding the above-referenced DUA, CMS wishes to allow the Department to use and, in certain circumstances, disclose the CMS data covered by that DUA in the context of the quality improvement project titled "HHS emPOWER Program Response Outreach" (hereinafter referred as "the Project"). In doing so, CMS wishes to authorize the Department to disclose such data to:

    a. entities acting under a formal delegation of authority from the Department whereby such entity is carrying out public health activities (as defined in 45 CFR 164.501) on behalf of the Department in the Project,
    b. another public health agency (working with the Department under their own public health authorities in the context of the Project),
    c. Entities with a "treatment" relationship (as defined in 45 CFR 164.501) with individuals participating in the Project.

    In doing so, CMS intends to allow all such parties to use such data in accordance with the terms of the above referenced DUA, as modified by this addendum, to identify vulnerable individuals who may need health assistance prior to, during, and in the aftermath of an incident, emergency, or disaster that poses an adverse health and/or public health impact, and to plan for and provide assistance during such events. In accepting such use and disclosure authorities, however, the Department affirms that it will ensure that it, and those to whom it discloses such data, will limit access to such data to the minimum data necessary to achieve the purpose of the project (i.e., individual's access to the data will be on a need-to-know only basis).

2. Notwithstanding section 2 and 3 of the DUA referenced above, but subject to the following paragraph (limiting use of CMS or derivative data to populate registries), those entities that receive data under that DUA (i.e., the Department) or by virtue of the preceding paragraph may retain any CMS data or any derivative data if such data is:

    a. The only source for that entity's legally required records, such as instances in which record retention laws apply to the data in the hands of a state (including political subdivisions within the state) actor, or where medical record requirements mandate the data's inclusion in a patient's medical record. In

determining whether records are legally required, such parties shall rely upon the definition of "required by law" under the HIPAA Privacy Rule, 45 CFR 164.103. However, if such laws include expiration dates for such data retention obligations, the CMS data and any derivative files shall be destroyed within 30 calendar days of that date.

b. Maintained in a HIPAA covered entity's designated record set (i.e., when such data qualifies as Protected Health Information (PHI) as defined at 45 CFR 160.103, and is therefore protected by the HIPAA Privacy and Security Rules). This provision applies equally to PHI in the hands of such covered entities' business associates so long as such records qualify as PHI under HIPAA.
c. Maintained by a state (including political subdivisions within the state) actor in a data system that is subject to privacy laws equivalent to or more stringent than the requirements imposed on Federal actors holding similar records under the Privacy Act of 1974.
d. As otherwise permitted in writing by the Centers for Medicare & Medicaid Services.

3. Except as provided in this paragraph, no CMS data or derivative data that is subject to the above-referenced DUA or this addendum may be entered into a registry. Notwithstanding the prior two paragraphs and in accordance with the preceding sentence, in instances in which a registry predating the Project is relevant to an individual served by the Project, those providing treatment in the context of the Project, or carrying out public health activities under the authority of a public health authority operating under the Project may, during course of delivering those services under the Project, offer the individual being served an opportunity to opt-in to participating in such registry, and, if the individual does opt-in, assist such individual in registering with such registry. But, in no instance may such entities contact an individual solely to offer or encourage participation in such registry, and in no instance should an individual who declines to opt-in be contacted a second time by such treatment/public health actors in the course of the Project in an attempt to change the individual's mind.

4. Notwithstanding sections 6 and 9 of the above referenced DUA, and subject to paragraph 2 of this addendum, the Department and any entities who receive data under paragraph 1 of this addendum may generally only retain the CMS source data received under the above-referenced DUA and/or any derivative data for a period of **30 calendar days**, hereinafter known as the "Retention Period. In the event the public health activities are expected to extend beyond the expiration of the Retention Period, the Department may submit an official written request on its own or its downstream data recipients' behalf for CMS's review and determination. All CMS data obtained under the above-referenced DUA and any derivative files that do not meet the conditions of paragraph 2 above must

be destroyed in accordance with CMS' protocols within 30 calendar days of the end of the Retention Period, which shall be termed the Destruction Date. The Department shall provide CMS with a written attestation confirming its destruction of all data subject to this DUA, as amended, including any derivative data and/or any copies distributed in accordance with paragraph one that are not subject to paragraph 2 by the Destruction Date.

5. The Department also agrees to bind downstream data recipients of CMS data or derivative data to the terms and conditions of the DUA, as amended (including but not limited to the privacy and security, minimum necessary access, retention and destruction provisions) prior to providing such downstream entities access to, or copies of such data. In doing so, the Department shall take appropriate administrative actions to ensure that such entities are vetted and/or credentialed as being capable of using and/or disclosing such data only as provided under this DUA, as amended. Such efforts shall include at a minimum:

    a. Ensuring that those carrying out the project that will have role-based access to CMS data or any derivative data do not have a criminal background that would suggest that such individual could be a risk to those served by the Project.
    b. Clearance and/or approval under any applicable laws policies, and or protocols for access to the Department's sensitive data.
    c. Privacy and security training, including HIPAA training where required by virtue of their being granted access by virtue of their working on behalf of a HIPAA covered entity or its business associate.
    d. A binding agreement with the Department that holds the entity to the terms and conditions in the above-referenced DUA including a statement that their access to and use of the project's CMS source data and any derivative data is provided to allow them to perform specified public health activities under the project and a reminder that the CMS source data and any derivative data must be destroyed (and verified via attestation provided to the Department) unless retention is permitted under paragraph 2 above.

6. Notwithstanding the second sentence of section 7, or sections 9, 10, and 11 of the DUA, the Department and any data recipients under paragraph 1 above shall not be required to establish safeguards at the specified levels so long as they employ appropriate administrative, technical, and physical safeguards to protect the confidentiality of the CMS data and/or derivative data. Such protections shall include, but not be limited to measures that prevent unauthorized use or access to or use of such data. Such protections may include, but would not be limited to logon protocols and passwords for electronic access to such data, encryption of such data at rest and in transit, permanent deletion of internet histories when using third party resources, and redaction of information when

fully identifiable information is not required, and the use of sufficient overwriting to ensure permanent deletion of electronic copies of such data or the physical destruction of such data in accordance with paragraph two above.

7. Data Incidents/Breaches. The Department shall notify CMS of any actual access, use, or disclosure of CMS data or any derivative data that is not in accordance with the terms of the above-referenced DUA as modified. This includes forwarding reports of such violations from all downstream users to whom the Department provides such data received under the DUA with one (1) business day of discovering the breach.

8. Except as specifically modified and amended herein, all terms, provisions, requirements and specifications contained in the above-referenced DUA remain in full force and effect.

The effective date of this addendum to the above-referenced DUA is the date when the addendum is fully executed.

_____
Tracy S. Gruber
Executive Director
Utah Department of Health and Human Services

_____
CMS Representative