Health Resources and Services Administration:
HIV/AIDS Bureau Client Level Data System

1. It is not clear whether HRSA's de-identification methodology meets the requirements of the HIPAA privacy rule because it contains the date of birth and a unique identifying number. Can you please clarify? Here's what the rule requires:

The Privacy Rule makes two methods available for de-identifying health information:

a. Remove the 18 specific identifiers listed in the Privacy Rule and determine there is no other information that may identify the individual. The identifiers are:
   - names
   - geographic subdivisions smaller than a state
   - all elements of dates (except year) related to an individual (including dates of admission, discharge, birth, death and, for individuals over 89 years old, the year of birth must not be used)
   - telephone numbers
   - FAX numbers
   - electronic mail addresses
   - Social Security numbers
   - medical record numbers
   - health plan beneficiary numbers
   - account numbers
   - certificate/license numbers
   - vehicle identifiers and serial numbers including license plates
   - device identifiers and serial numbers
   - web URLs
   - internet protocol addresses
   - biometric identifiers (including finger and voice prints)
   - full face photos and comparable images
   - any unique identifying number, characteristic or code

b. Obtain an opinion from a qualified statistical expert that the risk of identifying an individual is very small under the circumstances; the methods and justification for the opinion should be documented.

The client level system collects service dates and year of birth only, and a unique identifier is generated using a standard approved by the Department of Commerce for use by federal departments and agencies for the protection of sensitive unclassified information. The Privacy Rule requires de-identification of information for research purposes using the elements listed above; however, de-identification of information is not required under the public health provision when covered entities are reporting to a public health authority. HRSA requires service dates to determine if clients are receiving the clinical services with the frequency and spacing that are considered necessary to

meet minimum standards of HIV care. Date of first service from a provider is important in order to identify new clients; one of our PART measures requires us to report the number of "new clients" who had a viral load and CD4 count lab test. HRSA's supporting statement language stated that this client level data collection was in compliance with HIPAA's de-identification requirements, and we will make appropriate revisions to correct and clarify this issue.

The HHS/Office of Civil Rights provides the following information regarding HIPAA and privacy on its web site:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/publichealth/index.html

Covered entities may disclose protected health information to public health authorities pursuant to the public health provision. By way of background, a covered entity may disclose protected health information (PHI) without the patient's authorization to a public health authority that is legally permitted to collect or receive such information for public health surveillance or related activities (45 CFR 164.512(b)(1)). Various Department of Health and Human Service (HHS) agencies, such as National Institutes of Health (NIH), and the Health Resources and Services Administration (HRSA), are authorized by law to assist the Secretary of Health and Human Services in carrying out the purposes of section 301 of the Public Health Service Act. Those agencies are public health authorities under the Rule, even if they have other non-public health mandates.

The legislative language in 45 CFR 164.512(b)(1) states:

> b) Standard: uses and disclosures for public health activities. (1) Permitted disclosures. A covered entity may disclose protected health information for the public health activities and purposes described in this paragraph to:
> (i) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

OMB: Thank you for this clarification. It seems that the privacy rule does allow the disclosure of PHI to HRSA, but it seems like HRSA should not be describing this data as "de-identified." Can HRSA revise the supporting statement and instructions to clarify this?

HRSA: Yes, the instructions can be revised to more clearly state that the data are not de-identified under HIPPA Privacy Rule. HRSA assures OMB that the language will be revised before the client level data system is fielded.

Although the information from grantees will include dates of service, HRSA will not obtain other personally identifiable information (birth date, name, SSN, etc.); however, a unique identifier must be used for the patient records to avoid duplication of client information. To meet the highest federal standards for privacy and security, HRSA's HIV/AIDS Bureau selected the Secure Hash Algorithm (SHA-1) algorithm as the encryption technique for the Ryan White client level data. Developed by the National Security Agency and published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard, the SHA-1 algorithm is commonly used in government and by private institutions deeply concerned with client privacy and data security. With use of this encryption method and associated security applications, combined with the removal of all personal identifiers other than service dates, HRSA is able to provide assurances that the information obtained from funded service providers will be secure.

OMB: We thought that the client's date of birth (and gender) make up the unique client ID. Does HRSA's response mean that this UCI is encrypted with SHA-1 before it is sent to HRSA? So HRSA will never actually see the date of birth and gender information that make up the UCI?

HRSA: Yes, that is correct. HRSA will not ever see the actual date of birth, social security number or other sensitive information that make up the Unique Client Identifier.

2. The response to comments seems to imply that HRSA will be requiring the collection and reporting of duplicative data – the HAB client level data as well as the current reporting requirements. Because this is a new and big endeavor that will have PART implications, we can understand why HRSA will want to ensure the quality of the information collected through the HAB client level data system. It also sounds like HRSA is proposing to do this for the first year only and, presumably, assess whether any changes are required of the HAB client level data system. Is this correct? If so, would HRSA be amenable to an abbreviated 18 months clearance? OMB is willing to approve this duplicative information collection as long as it is (a) for a finite period of time and (b) as long as the purpose of the duplication is to ensure data quality.

No changes are anticipated for the client level data system in the next few years. The submission of both the client level data and the current reporting requirements is for the purpose of ensuring that HRSA continues to receive complete information on services provided while implementing the new system. Only a portion of service providers will report in the first year; therefore, HRSA will still need the aggregate information currently provided. This will permit an assessment of the quality of the

information provided and technical assistance needed. HRSA would be amenable to an approval period of 24 months, as this would cover the two calendar years of data collection and reporting. A shorter approval period would interrupt the second year of data collection and reporting. The only revisions anticipated during the two year implementation are clarifications to instructions, and additional requirements for technical assistance or training.

OMB: So to clarify, after 24 months, the respondents will no longer have to fill out the current reporting requirements? After 24 months, they will only have to report the client level data?

HRSA: Yes, this is correct.

3. Relatedly, has HRSA considered requiring a sample of respondents to fill out both sets of data – the current reporting requirements as well as the new HAB client level data—rather than requiring the universe of respondents to fill out both sets of data? This might limit the additional burden/duplication to a smaller set of respondents while also allowing HRSA to assess where the data quality issues are.

Client level reporting is being phased in for funded grantees/providers over the 2009/2010 calendar years. In effect, this results in a sample of respondents for the calendar year 2009, since not all service providers will report the first year. (Only case management and medical care providers will report for 2009.) OMB is correct in that the first year will have a smaller set of respondents, and HRSA will be carefully reviewing respondent issues related to reporting and data quality. The 2010 calendar year will add the remaining providers to the reporting system.

4. Can HRSA clarify when it plans to begin using the HAB data for PART and GPRA purposes?

HRSA anticipates using client level information from calendar year 2010 to re-evaluate targets for the program for performance reporting and GPRA, and data from calendar year 2011 will be used for PART.

OMB: so just to clarify, is this the anticipated time table?
HRSA: Yes, this is the anticipated timetable. We have added some brief notes for further clarification. A minimum of a 24-month clearance is needed to allow full-year collection and reporting since grantees do not report until spring of the following calendar year.

CY 2009	First year of OMB clearance	Case Management and Medical Providers Report in Spring 2010 on CY 2009 Data
CY 2010	Second year of OMB	First year of full data for Client-level

	clearance; OMB approval expires for the aggregate level reporting system (RDR) in spring 2011.	system from all HAB providers. CY 2010 not reported until Spring 2011
CY 2011	ICR will be renewed; data collected during this year will be reported for the PART in 2012	Previous reporting requirements for aggregate data are discontinued.
CY 2012	Client level data will be used for PART based on CY 2011 data	Client level data will be used for PART based on CY 2011 data