

November 10, 2010

The Honorable Kathleen Sebelius
Secretary
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Madam Secretary:

Re: Recommendations Regarding Sensitive Health Information

The National Committee on Vital and Health Statistics (NCVHS) is the Department of Health and Human Service's statutory public advisory body on health data, statistics, and national health information policy. The NCVHS has historically made recommendations about health information privacy, confidentiality, and security, and has responsibility under federal law for making recommendations to HHS on the Health Insurance Portability and Accountability Act (HIPAA).

Based on the Committee's collective hearings and deliberations in recent years, we are writing to recommend that HHS explore the use of technology that can assist with the management of sensitive health information. Such analysis is critical to inform effective policy development around this central topic. Our nation is committed to deploying interoperable health records to improve patient health, health care, and public health. Patient trust is critical to patient participation in this deployment, and, therefore, we must invest in technologies that will promote this trust.

The sensitivity of data is often influenced by the context in which it appears. The ability to transfer health information with contextual data restrictions is an important part of the trust relationship. In order for such restrictions to be meaningful, a key strategy is the identification of categories of sensitive information that can be assigned special handling. In this letter, NCVHS suggests certain defined categories of sensitive health information. Federal and state laws already require special handling for certain defined categories of sensitive information in particular contexts; other categories may also need to be identified to satisfy patient privacy concerns. NCVHS recognizes that multiple approaches to the protection of sensitive data may eventually be needed.

For example, individual pieces of data, not necessarily in conventionally sensitive areas, may also be considered sensitive. Furthermore, some pieces of data included in sensitive categories may not be considered sensitive by some patients.

Congress in the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, NCVHS in prior letters, and the Health Information Technology Policy Committee (HITPC, an advisory committee to the Office of the National Coordinator for Health Information Technology (ONC)) all have recommended identifying categories of sensitive health information. The HITECH Act specifically directed the HITPC to make recommendations for:

technologies that protect the privacy of health information and promote security in a qualified electronic health record, including for the segmentation and protection from disclosure of specific and sensitive individually identifiable health information with the goal of minimizing the reluctance of patients to seek care (or disclose information about a condition) because of privacy concerns, in accordance with applicable law...

Investment in electronic health records and health information exchange is proceeding rapidly; attention to this issue is urgently needed to protect individuals and to obtain the returns to patient care and health research that are hoped for from investments in health information exchange and the NHIN.

Based on NCVHS's past work concerning sensitive information, we are now offering initial definitions of categories of sensitive information. These recommendations coordinate with the work of the Health IT Policy Committee, which is separately addressing the technical requirements in this area and has held hearings on that facet of the topic. In a September letter to Dr. David Blumenthal, the Health IT Policy Committee noted the importance to patients of controlling transfers of sensitive information and stated that meaningful granular consent "must be generated out of further innovation and, critically, testing of implementation experience"¹ as it pertains to policies related to electronic exchange of health information.

The discussion and recommendations in this letter continue to be based on the same critical considerations as in prior letters: protecting patients' legitimate concerns about privacy and confidentiality, fostering trust and encouraging participation in health information exchanges, improving patient care, promoting innovation in health information technology, and protecting the integrity of the health care system. They are

¹ Health IT Policy Committee, Letter to David Blumenthal, National Coordinator for Health Information Technology, Sept. 1, 2010, p. 8.

also based on NCVHS's commitment to the advancement of health data stewardship² and the policy and scientific advancement of health statistics.

Below, we present our recommendations and discuss our reasoning in more detail.

Recommendations

NCVHS recommends that HHS

1. Conduct an environmental assessment of current capabilities of electronic health records and health information exchanges to identify and manage sensitive information;
2. Compile and publish best practices and existing standards, if any, for the identification and management of categories of particularly sensitive information;
3. Invest in research to enhance the capabilities of electronic health records and health information exchanges to identify and manage sensitive information, including the development of standards, if appropriate;
4. Invest in pilot tests and potential future demonstration projects to assess the technological feasibility, effects on patient care, efficacy for privacy protection, benefits and costs, and other previously unidentified consequences of these capabilities.
5. Include the following in its research and pilot tests:
 - a) Categories already identified in federal law that require special handling;
 - b) Categories already identified in state laws that require special handling; and
 - c) Additional categories defined in this letter that emerged in NCVHS hearings.

NCVHS Prior Study of Sensitive Health Information

NCVHS has held nine hearings relevant to the topic of sensitive information over a six-year period: four hearings on "Privacy and Health Information Technology" in 2005, three hearings on "Privacy Protections for Medical Records of Non-Covered Entities" in 2006 and 2007, a hearing on "Personal Health Records" in 2009, and the most recent hearing on "Sensitive Information in Medical Records" in June of this year.

² National Committee on Vital and Health Statistics, Health Data Stewardship: an NCVHS Primer, <http://www.ncvhs.hhs.gov/090930lt.pdf> (September 2009).

Based on these hearings, our collective expertise, and extensive deliberation, NCVHS has already made a number of recommendations concerning sensitive information. These earlier recommendations are:

Letter to the Secretary, “Recommendations regarding Privacy and Confidentiality in the Nationwide Health Information Network” (June 22, 2006). This letter recommended, first (R6): HHS should assess the desirability and feasibility of allowing individuals to control access to the specific content of their health records via the NHIN, and, if so, by what appropriate means. Decisions about whether individuals should have this right should be based on an open, transparent, and public process. Second, this letter recommended (R7): If individuals are given the right to control access to the specific content of their health records via the NHIN, the right should be limited, such as by being based on the age of the information, the nature of the condition or treatment, or the type of provider.”

Letter to the Secretary, “Individual control of sensitive health information accessible via the Nationwide Health Information Network for purposes of treatment” (February 20, 2008). After exploring the possibilities outlined in the 2006 letter (specification by age of the information, nature of the condition or treatment, or type of provider), in 2008 NCVHS recommended that categories of sensitive information be defined for purposes of health information that is made accessible over the NHIN for treatment purposes. The Committee also recommended that “[t]he design of the NHIN should ensure that when a health care provider accesses health information with one or more categories sequestered, a notation indicates that sensitive health information has been sequestered at the direction of the patient.” Moreover, the Committee included a “break the glass” feature for emergency situations, development of the technological capacity for re-sequestration after emergency access to sensitive information, and development of audit capability in cases of such access.

Our 2008 letter also recommended, “HHS should initiate an open, transparent, and public process to identify the possible categories of sensitive information” and “define with specificity the criteria for inclusion and exclusion within each category.” The process, NCVHS said, “should take into account both patient concerns about privacy and the concerns of health care providers about quality of care.” Our 2008 letter also listed these five “example categories” of sensitive information:

Domestic Violence,
Genetic information,

*Mental health information,
Reproductive health, and
Substance abuse.*

Letter to the Secretary, “Protection of the Privacy and Security of Individual Health Information in Personal Health Records” (September 28, 2009). This, most recent, letter extended the application of sensitive categories to personal health records (PHRs) recommending that “PHR products should be designed to allow consumers to identify designated categories of sensitive health information,” and that “the consumer should then have the ability to control the use and disclosure of the information in these sensitive categories (including in emergency situations).³

In the spring of this year, the Subcommittee on Privacy, Confidentiality, and Security noted that additional attention still needed to be given to these recommendations, and that such attention was important for the progress of the NHIN. We reviewed the written testimony and transcripts from the earlier hearings leading to prior recommendations and determined that it would be helpful to refine the categories of sensitive information and to be more explicit about what next step HHS should take. We conducted additional hearings on June 15, 2010, entitled “Sensitive Information in Medical Records,” selecting witnesses to fill in gaps where information was lacking from prior hearings.

Legally Defined Categories of “Sensitive” Information

Numerous federal and state laws require special treatment for specified categories of sensitive health information in various contexts. In these contexts, the records custodians may find it useful to have the capacity electronically to segregate these categories of information for special handling, to the extent possible, in order to comply with the law. Our recommendations 5a and 5b above refer to these legally recognized categories of sensitive information. We have included a discussion of certain common categories where state law mandates special handling, but these are only examples.

Categories Defined in Federal Law

Genetic information

The federal Genetic Information Non-Discrimination Act of 2008 (GINA)⁴ prohibits employers and certain insurers from “request[ing], requir[ing], or purchas[ing]” genetic information. Health care providers are regularly requested to provide medical records for a number of legitimate employment and insurance purposes. In order to respond to these requests, records custodians must segregate genetic information that comes

³ Letter to the Secretary, “Protection of the Privacy and Security of Individual Health Information in Personal Health Records” (September 28, 2009).

⁴ Pub. L. 110-223, 122 Stat. 881 (2008).

under the GINA definition from other parts of the electronic medical record when transmitting records.

The definition of genetic information in GINA is the most expansive definition in any current law; it includes not only genetic tests and the genetic tests of family members but also the “manifestation of a disease or disorder in family members.” “Genetic tests” include not only tests for DNA, RNA, or chromosomes, but also tests for metabolites or proteins that are indicative of genetic factors. The GINA definition excludes as genetic information diagnoses of genetic diseases and expressed conditions.

State law definitions may be more limited, extending in some cases only to tests for DNA, RNA, or chromosomes and in other cases to tests for proteins or metabolites that are indicative of genetic characteristics when the individual is not symptomatic for disease. Some state statutes, however, follow the more expansive GINA definition of “genetic information.”

Psychotherapy notes

Under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, a covered entity must obtain authorization for any use or disclosure of psychotherapy notes, with certain limited exceptions.⁵ Unlike the rest of the medical record, a health care provider may not disclose psychotherapy notes for treatment, payment, or health care operations without an explicit authorization. Furthermore, although patients have the right to review and obtain copies of their medical records, health care providers may exclude psychotherapy notes.⁶ HIPAA defines psychotherapy notes as:

notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. *Psychotherapy notes* excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.⁷

⁵ 42 CFR 164.508(a)(2).

⁶ 42 CFR 164.524(a)(1)(i).

⁷ 42 CFR 164.501. Some of the excluded items may be included within a larger definition of “mental health information,” discussed below.

In order to come within this definition, psychotherapy notes must be created by a mental health professional and separated from the rest of the medical record. Therefore, in order to avoid violating the law when disclosing records, and in order to exercise the discretion to withhold psychotherapy notes from the subject patient, it would be necessary for custodians of the medical record to create a separate psychotherapy notes section in the electronic health record to appropriately manage this part of the medical record.

Substance abuse treatment records

Federal regulations governing the confidentiality of alcohol and substance abuse treatment records impose “restrictions upon the disclosure and use of alcohol and drug abuse patient records which are maintained in connection with the performance of any federally assisted alcohol and drug abuse program.”⁸ Such a “program” might be an individual care provider, stand-alone facility, unit within a general medical facility, or medical staff of a larger medical facility who hold themselves out to provide alcohol or drug abuse diagnosis, treatment, or referral for treatment.⁹ These regulations also prohibit the re-disclosure of information that originated as substance abuse treatment records; in other words, the protections for these records attach to the record and not the custodian, as under HIPAA.

Especially for those medical staff or units within a larger care facility where medical record systems are integrated, the capability to identify and separately manage substance abuse records is critical to proper compliance with the law. But due to the prohibition on redisclosure, all entities that might possibly receive substance abuse treatment records are at risk of violation if they do not have the capability to identify these records separately. In the meantime, more than one witness testified before NCVHS that facilities who do not have this capability avoid integrating the records of substance abuse patients into their systems, requiring more than one system for maintaining records, and denying this population of patients other advantages of electronic medical records and health information exchange.

HITECH Act Cash Payments

Under the HITECH Act, patients may require that a provider withhold from a health insurance company information about any service for which the patient has paid in full out of pocket. In order to do so, records custodians will need to be able to separate out items or services for which the provider has been paid out of pocket in full.

Categories Defined in Laws of Many States

State law protections for HIV information, or other information regarding sexually transmitted diseases

⁸ 42 CFR 2.3(a).

⁹ 42 CFR 2.11.

Many state laws give special protections to information concerning testing, diagnosis or treatment for the Human Immunodeficiency Virus (HIV) or other sexually transmitted diseases. For example, New York law provides that “[n]o person who obtains confidential HIV related information in the course of providing any health or social service or pursuant to a release of confidential HIV related information may disclose or be compelled to disclose such information.”¹⁰ There are exceptions for disclosures authorized by the individual, disclosures that are required for treatment of the individual or others, and disclosures with respect to blood products. The definition of “HIV related information” is:

“any information, in the possession of a person who provides one or more health or social services or who obtains the information pursuant to a release of confidential HIV related information, concerning whether an individual has been the subject of an HIV related test, or has HIV infection, HIV related illness or AIDS, or information which identifies or reasonably could identify an individual as having one or more of such conditions, including information pertaining to such individual's contacts.”¹¹

In order to comply with New York law regarding disclosures of HIV-related information, custodians of health records may need to segregate information that comes within the different parts of this statutory definition.

It will not be easy to define a single category of “protections for HIV information or other information regarding sexually transmitted diseases,” because state laws vary in how they define these protections. Massachusetts prohibits disclosing the results of an HIV test or identifying anyone who has taken such a test “without first obtaining the subject’s written informed consent.” The same section prohibits employers from requiring an HIV test as a condition of employment.¹² Therefore, whenever the Massachusetts medical record is disclosed in a case that does not require consent, the HIV test information must be identified and separately handled to comply with the law. Every time a health care provider plans to respond to a legitimate request from an employer, the record must be checked to ensure no information about HIV testing appears in the record. It would be useful to have the capability to perform this function automatically.

Accordingly, it is important to be able to identify the types of information that might be included within this category, the contexts in which disclosure limitations might apply, and how the particular types of information might be identified for purposes of disclosure

¹⁰ New York Public Health Law 27-F.

¹¹ New York Public Health Law 27-F.

¹² Ann. L. Mass. GL ch. 111, § 70F

limitations in these various contexts. For example, under the New York statute, disclosure limitations differ when the information is required for treatment.

State law protections for mental health information

Most states give some kind of special protection to mental health information. For example, West Virginia applies special rules to protection of the confidentiality of mental health information. Under the West Virginia statute, “mental health information” is defined to include:

the fact that a person is or has been a client or patient, information transmitted by a patient or client or family thereof for purposes relating to diagnosis or treatment, information transmitted by persons participating in the accomplishment of the objectives of diagnosis or treatment, all diagnoses or opinions formed regarding a client's or patient's physical, mental or emotional condition, any advice, instructions or prescriptions issued in the course of diagnosis or treatment, and any record or characterization of the matters hereinbefore described.¹³

In Maryland, disclosures of mental health information are governed by law, and include a subsection regarding psychological test information. Maryland law explicitly requires contextual access disclosures for mental health records. It says that when a mental health record is disclosed “without the authorization of a person in interest, only the information in the record relevant to the purpose for which disclosure is sought may be released.”¹⁴ Unlike HIPAA, Maryland law does not require the minimum necessary information, but it limits the information to that which is “relevant.” In Texas, the law prohibits disclosure of the records of state mental health facilities that directly or indirectly identify a current, former or proposed patient.¹⁵ Georgia permits a provider to withhold mental health records from the patient, but never defines mental health records except to refer to them as “psychiatric, psychological or other mental health records of an individual.”¹⁶

State statutes vary in the definitions of mental health information to which they accord special protection, as well as in the contexts to which these protections apply. Accordingly, it is important to identify the types of information that might be included within this category, the contexts in which disclosure limitations might apply, and how the particular types of information might be identified for purposes of disclosure limitations in these various contexts. For example, under the West Virginia law,

¹³ W. Va. Code § 27-3-1.

¹⁴ Md. Health-General Code Ann. § 4-307(c) (2010).

¹⁵ Tex. Health & Safety Code § 576.005.

¹⁶ OCGA § 31-33-4.

disclosure limitations differ when the information is needed to protect the patient against a clear and substantial danger of imminent injury to self or others.

State law provisions regarding access to information in the records of children and adolescents.

State laws differ regarding the rights of adolescents and their parents to the health records of adolescents. For example, Idaho provides special rules with respect to access to the records of children who have received involuntary mental health services. These limits include: “No person in possession of confidential statements made by a child over the age of fourteen (14) years in the course of treatment may disclose such information to the child's parent or others without the written permission of the child.”¹⁷ There are limits to this restriction in some contexts: disclosures that are “such disclosure is necessary to obtain insurance coverage, to carry out the treatment plan or prevent harm to the child or others, or, unless authorized to disclose such information by order of a court.” Adherence to this restriction may require separate handling of records of involuntary mental health services received by children over 14. Indeed, many of the categories of sensitive information discussed in this letter may require separate handling in the case of adolescents in some states.

Without the capacity for separate management, however, even where electronic medical records are in place, responses to requests for release of this information often requires that the records be manually redacted. This process is inefficient, cumbersome, and expensive. Alternatively, custodians may be forced to withhold information from health information exchanges when they would not otherwise do so, because they lack the capacity to differentiate the sensitive portion of the record. For example, a psychiatrist may fail to include any mental health records, or physicians may avoid placing records of treatment for adolescents in electronic record systems because they are unable to segregate the sensitive portions of the record. In such cases, patients lose the benefits of both EHRs and exchange, and other uses of the information (such as for public health or quality improvement) may also be frustrated.

We note that this is by no means a complete list of categories of sensitive information that have been identified in federal or state law. It represents, however, categories that witnesses at our hearings called to our attention as especially important or frequently protected by legal requirements.

Additional Potential Sensitive Categories of Information

NCVHS heard extensive testimony about the definition of sensitive categories of health information that extend beyond these categories and have found legal recognition. These were categories that were singled out for protection in at least some contexts, or

¹⁷ Idaho Code § 16-2428 (2010).

in a broader way than the statutory requirements provide, as important to maintaining patient trust. What follows are two of these categories, together with information that may be important in defining them.

Mental health information (other than as found in HIPAA psychotherapy notes or state law definitions)

Dissemination of information about mental health diagnosis and treatment may pose significant risks to patients, and most people regard it as highly sensitive. However, the distinction between mental and physical health is regarded as artificial; witnesses and members of the Committee “welcomed the day” when this information would no longer need to be singled out for special concern.

One definition of “mental health information” recommended to us in testimony is “information gathered or observed relating to a person’s emotional, perceptual, behavioral or cognitive experience, as well as associated physical symptoms.” This definition is consistent with the definition of mental health information found in some state laws. Some of this information, however, may be difficult to identify as it will be scattered throughout many parts of a medical record, as well as across many providers’ records and might require the use of advanced natural language processing for identification. Additionally, medical notes, tests, procedures, imaging or laboratory studies performed in a mental health facility that would otherwise be considered medical data—such as evaluation for reported chest pain by a patient in a psychiatric facility—should not be included in “mental health information.”

NCVHS heard testimony that, mental health diagnoses, patients’ descriptions of traumatic events relating to their mental health, a past history of mental health treatment, educational testing and testing for attention deficit disorder should also be included in the category of mental health information to be segmented.

On the other hand, NCVHS also heard testimony about the importance of some mental health information to treating the patient for non-mental health related issues. One panelist recommended that the following “critical mental health information” should not be included within the category of mental health information to be segmented in the record: medication lists, allergies, non-allergic drug reactions, and dangerous behavior within medical settings. Information about current medications is crucial to avoid drug/drug interactions. Another expert suggested the importance of a problem list to current care; for example, knowledge of alcohol abuse, may be relevant to diagnosis and treatment in an emergency setting. Our witnesses emphasized that this information may need to be available in emergency settings or when patients with mental health diagnoses are being treated for other conditions.

In addition to the statutory requirements in state law for mental health, and psychotherapy notes at the federal level, NCVHS believes the category of mental health information includes:

- Psychiatric diagnoses
- Descriptions by patients of traumatic events
- Descriptions or analyses of reports by the patients of emotional, perceptual, behavioral, or cognitive states

Except as required by state law, NCVHS does not believe the following “critical health information” should be included in additional definitions of “mental health information” because of its importance in many contexts:

- Medication lists
- Allergies and non-allergic drug reactions
- Dangerous behavior within medical settings
- Information from medical notes, tests, procedures, imaging or laboratory studies performed in a mental health facility that is not related to the mental health treatment but that would otherwise be considered medical information, such as cardiac studies to diagnose reported chest pain

NCVHS heard conflicting testimony regarding whether or not information about a psychiatric diagnosis should itself be included within the category of sensitive mental health information. While this information may be important for patient care, it may be very sensitive to patients and they might expect it to be included within the category of mental health information.

Sexuality and Reproductive Health Information

Information about sexuality and reproductive history is often very sensitive. Some reproductive issues may expose people to political controversy (such as protests from abortion opponents), and public knowledge of an individual’s reproductive history may place him or her at risk of stigmatization. Additionally, individuals may wish to have their reproductive history segmented so that it is not viewed by family members who otherwise have access to their records. Parents may wish to delay telling their offspring about adoption, gamete donation, or the use of other forms of assisted reproduction technology in their conception, and, thus, it may be important to have the capacity to segment these records.

With regard to Recommendation 5(c), NCVHS believes the following elements comprise the category of Sexuality and Reproductive Health Information:

- Sexual activity
- Sexual orientation

- Gender dysphoria and sexual reassignment
- Abortion, miscarriage, or past pregnancy
- Infertility and use of assisted reproduction technologies
- Sexual dysfunction
- The fact of having adopted children

Some of this information, for example sexual orientation discussions, may be especially sensitive in adolescent records if they are accessible to parents under state law.

Considerations Applying to Entire Records

NCVHS has identified three circumstances in which the entire record might be deemed “sensitive” requiring some notation that would permit it to be handled in order not to identify the record subject other than to the immediate health care providers who are caring for the patient.

First, in cases of domestic violence or stalking, identification of the fact that the record exists with a given provider might provide an abuser or stalker with the information necessary to locate a potential victim. So might information in the record that is usually not sensitive, such as the patient’s address, place of employment, school, or the number and ages of her children. NCVHS heard testimony from victim protection organizations of cases in which the medical record served to provide the victim’s address or indicate the area in which the victim had sought treatment and thus was likely to be found; in several of these cases, the result was the tragic death of the victim who did not realize that her record had been accessed for this purpose.

Second, there are cases in which the identity of a patient being treated is sensitive, and identification of the record might serve to reveal that treatment has occurred, or invite speculation, harassment, or undesired attention. Public figures and celebrities might come within this category.

NCVHS is aware that it is sometimes desirable to mask the identity of victims of violent crime who present in the emergency room so as to avoid security incidents. For example, gunshot victims are routinely assigned pseudonyms upon admission to urban hospitals so that the perpetrator does not come looking for the victim to “finish the job,” endangering all of the patients, the hospital staff, and visitors to the hospital.

Finally, NCVHS heard testimony that the records of adolescents may require special treatment with respect to access and thus that it may be particularly important to be able to segment parts of these records. While state laws vary concerning parent/guardian and adolescent access to an adolescent’s medical records, typically certain aspects of the adolescent’s medical record are considered sensitive, such as the categories described in this letter. Adolescents may not wish their reproductive information,

sexually transmitted disease information, information about mental health treatment, or substance abuse information shared with their parents. The laws of some states give adolescents legal rights that particular types of information not be shared as they would for younger children with a parent or guardian. In addition, NCVHS heard testimony that it may be important for records of this type not to be transferred back to a primary care provider for the adolescent if there is a risk that they might be shared with the parents even though the records would not have been shared directly. NCVHS also heard testimony that patients might wish to segment certain types of records created during their childhood, for example a history of enuresis, learning disabilities, or testing for attention deficit disorder. In the absence of the ability to identify adolescent records or records created during childhood, the use of EMRs and their interchange is likely to prove particularly challenging for providers of health care to this population. Therefore, records of minors may need to be identifiable as such.

Conclusion

NCVHS recommends that HHS use the above categories of sensitive health information as a basis for research, technical development, pilot testing, and potential future demonstration projects. Aims of these investments should be to understand the feasibility, need for technical standards, effects on patient care, efficacy for privacy protection, benefits and costs, and other possible consequences of segmenting these categories and implementing granular patient consent for their use in particular contexts. We also recommend that the Secretary undertake further research to explore other methods, in addition to those based on categories, of protecting sensitive data. NCVHS stands ready to help HHS in these continued and urgent endeavors.

Sincerely,

/s/

Justine M. Carr, M.D.
Chairperson,
National Committee on Vital and Health Statistics

cc:

James Scanlon
HHS Data Council Co-Chairs