Centers for Disease Control and Prevention (CDC)
Agency for Toxic Substances and Disease Registry (ATSDR)

Summary Report: February 7, 2007

Workshop on Human Subjects Protection (IRB) and Health Information Portability and Accountability Act (HIPAA):

Issues Related to Developing a National Surveillance System and Registries for Amyotrophic Lateral Sclerosis (ALS) and Multiple Sclerosis (MS)

Table of Contents — February 7, 2007

Introduction

February 7, 2007

The Agency for Toxic Substances and Disease Registry (ATSDR) has had an interest in surveillance for selected neurological and autoimmune diseases because of the lack of information necessary to answer community concerns about the incidence and prevalence of these diseases. In September 2002, ATSDR held a series of expert panels to begin exploring issues related to the design and maintenance of a successful surveillance system for selected neurological and autoimmune diseases. In March of 2006, a workshop was held to specifically discuss surveillance for multiple sclerosis (MS) and amyotrophic lateral sclerosis (ALS). MS and ALS were selected as the focus of the surveillance effort because of the large number of databases and research registries that already existed for these two diseases. At this meeting, a strategy of coordinating these extant groups to create a large database was discussed. In July 2006, ATSDR continued to advance the goal of surveillance systems for MS and ALS by funding five pilot projects, three in ALS and two in MS, which would attempt to implement a surveillance system for a defined geographic area. Information gained from these pilot projects would be used to guide the national effort.

The issues of human subjects protection and privacy have major implications for the success of such a strategy for a surveillance system. Therefore, it was decided to hold this workshop to discuss issues related to Human Subjects Protection (IRB) and the Health Insurance Portability and Accountability Act Privacy Rule and their implications for how the surveillance system might be structured.

Purpose and Call to Order — February 7, 2007

The purpose of this workshop was to discuss: 1) human subjects protection and privacy issues related to the development of surveillance systems and registries for Amyotrophic Lateral Sclerosis (ALS) and Multiple Sclerosis (MS); and 2) strategies for developing the surveillance systems and registries within the regulations for human subjects protection and privacy.

Dr. Wendy Kaye called the meeting to order, welcoming those present and thanking them for their participation. After reviewing housekeeping issues and travel arrangements, she introduced Dr. David Williamson.

Welcome — February 7, 2007

G. David Williamson, PhD
Director, Division of Health Studies
Agency for Toxic Substances and Disease Registry

Dr. Williamson expressed the Agency for Toxic Substances and Disease Registry's (ATSDR's) gratitude for the efforts the participants have made during the many years they have been working in the area of autoimmune and neurological diseases. He expressed his hope that they would get to know each other better, indicating that the agency looked forward to their guidance as they attempted to work collaboratively to beat these terrible diseases.

Acknowledging that many of the participants have had these diseases on their minds for many years, Dr. Williamson noted that ATSDR has also been giving a great deal of thought to ALS, MS, and other neurological and autoimmune diseases over the last five years. This effort is unparalleled in this field and is of such magnitude, he stressed that it would take all of them working together for several years to make the in-roads they believe they can make. He pointed out that the different disciplines and background they all brought to table was a reminder of how public health works, as well as a reminder that not only does it take the science of the medical field, but also in this project, the science of information technology (IT) and data collection, identification of all of the data available, and data editing. Then they must determine from an IT standpoint how they can utilize that data, and from a scientific standpoint how they can leverage resources to minimize the overlap and maximize the efficiency in the data they have.

Dr. Williamson invited the participants to let ATSDR staff members know what they could do to help them in their endeavors and he assured them that ATSDR looked forward to continuing to think about this project. In thinking about any kind of diseases and conditions that affect people so tragically and terribly, they cannot lose site of what it means to these individuals personally. At the same time, they have an obligation to them with respect to a privacy, confidentiality, and security standpoint. In addition to handling privacy, confidentiality, and security issues in accordance with the law, they also must do so in a way that is professional in terms of how they analyze and put together the data.

In conclusion, Dr. Williamson predicted that perhaps in five years they could reflect back, not just on this workshop or last March's workshop, but on the efforts that they have laid over the last year and a half that will have made a difference.

Overview of the Project and Goals — February 7, 2007

Vikas Kapil, DO, MPH
Chief, Surveillance and Registries Branch
Division of Health Studies
Agency for Toxic Substances and Disease Registry

Dr. Kapil provided a background and overview of how ATSDR reached this point with respect to developing a national surveillance system and registries for ALS and MS. In 2006, ATSDR was directed by Congressional language to create a national ALS registry. ATSDR has had some involvement for a number of years studying MS, ALS, and some other autoimmune diseases, particularly in relationship to hazardous waste sites. Because of that previous work and ATSDR's role in developing and creating surveillance systems and registries, they were asked to take this project on.

ATSDR held a workshop in March 2006 to discuss creating a national surveillance system for selected neurological and autoimmune diseases; identifying existing registries and databases; selecting disease(s) appropriate for surveillance activities; and developing and testing methodology related to that type of development work. That workshop resulted in a number of decisions. One of the major decisions was to begin the work with ALS and MS, and they decided to move forward in securing funding for pilot projects related to those two diseases. They discussed obtaining access to existing national data sets, which everyone thought would be an important step. They also considered developing and funding some pilot projects.

Approximately a year later, there has been remarkable progress. ATSDR obtained funds from two different sources to fund both ALS and MS pilot projects; developed statements of work for the pilot projects; and ultimately funded five pilot projects, three of which are on ALS and two of which are on MS.

ATSDR thought there would be significant economies of scale and advantages of conducting projects in ALS and MS concurrently. Obviously, there would be monetary savings. For example, data from the Centers for Medicare & Medicaid Services (CMS) would have been twice as expensive if requested separately. Moreover, preparing the data requests is not an easy task and is also expensive and time-consuming. Also extremely beneficial is having a brain trust of people. They have a number of scientists in the division who have been working on similar issues related to data for both ALS and MS. Having more people working on similar issues allows for sharing of ideas.

Dr. Kapil indicated that the purpose of this workshop was to consider one of the major issues for the use of existing data—human subjects protection and privacy. With that in mind, the plan was to discuss the regulations governing Institutional Review Boards (IRBs) and the Health Insurance Portability and Accountability Act (HIPAA); discuss different perspectives on the regulations; and discuss strategies for working within the regulations to develop surveillance projects and registries. With respect to data they have been able to obtain, for example from CMS and Veterans Administration (VA), these are large data sets with identifying information. There are many issues pertaining to use of this data for the purposes ATSDR has been discussing (e.g., determining cases of a particular disease), and working with the pilot projects, which are also looking at different methodologies to find cases.

Given the numerous issues concerning how these data should be managed and human subjects issues, ATSDR thought it would be useful to bring together a group of individuals with significant expertise in this area to discuss: regulations that govern IRBs (within the government and outside); HIPAA issues; and most importantly, strategies for working within the regulations to develop surveillance projects and registries in the future. Not only is this very important for the projects at hand, but also it has broader implications for other work in which ATSDR engages.

The HIPAA Privacy Rule: Scope, Structure, and Implementation — February 7, 2007

James G. Hodge, Jr., J.D., LL.M.
Associate Professor, Johns Hopkins Bloomberg School of Public Health
Executive Director, *Center for Law and the Public's Health*
Core Faculty, Berman Bioethics Institute

Professor Hodge discussed the basic principles of health information privacy, confidentiality, and security; assessed the existing universe of legal protections for the privacy and confidentiality of health data; examined the scope, structure, and implementation of the HIPAA Privacy Rule; discussed the impact of the HIPAA Privacy Rule on public health authorities; and explored the distinctions between public health practice and public health research for the purposes of applying privacy laws and policies. He stressed at the outset of his presentation that his intent was not to assess all of the potential privacy barriers, but

instead was to focus on how public health could carry out its work consistent with privacy rules. He also stressed that while he would focus on the Privacy Rule, there was a host of additional privacy laws in various jurisdictions of which they must be cognizant and compliant. Participants were referred to two articles in their packets summarizing the privacy laws outside the Privacy Rule, as well as the Center for Disease Control and Prevention's (CDC's) cleared guidance pertaining to the impact of the Privacy Rule on public health authorities.

With respect to key legal terms, although they are often used interchangeably, there are distinctions between *Privacy*, *Confidentiality*, and *Security*: 1) Privacy is an individual's right to control their identifiable health information in the broadest perspective; 2) Confidentiality concerns privacy interests that arise from a specific relationship (e.g., doctor / patient, researcher / subject) and corresponding legal and ethical duties; and 3) Security regards technological or administrative safeguards or tools to protect identifiable health information from unwarranted access, use, or disclosure. Professor Hodge shared the following quote from Willis Ware because it offers a good way to frame these various perspectives accurately: "If the security safeguards in an automated system fail or are compromised, a breach of confidentiality can occur and the privacy of data subjects invaded."

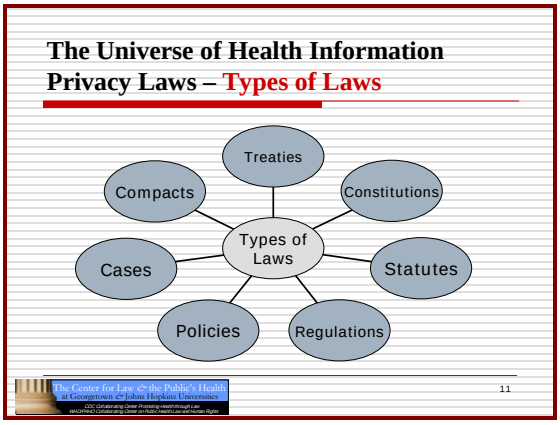
Most people appropriately think first about what can be done to restrict disclosures. While this is a core concept of privacy, it is not the only one. They must also be cognizant of three other major factors that are built into the Privacy Rule as well as a lot of the privacy laws. It is not just about how records are properly disclosed, but also is about how they are acquired, used, and stored. Privacy violations and infringements can come from unlawful acquisitions of data. If data is acquired for an ALS surveillance system, but is then used for purposes completely unrelated to surveillance of that disease across the nation, this constitutes a privacy violation. The data may be acquired lawfully, used in the manner intended, and not disclosed in any inappropriate way. However, if it is stored in a haphazard fashion on a laptop that is stolen from someone's trunk, there is now a storage related issue, a security concern, and a privacy violation.

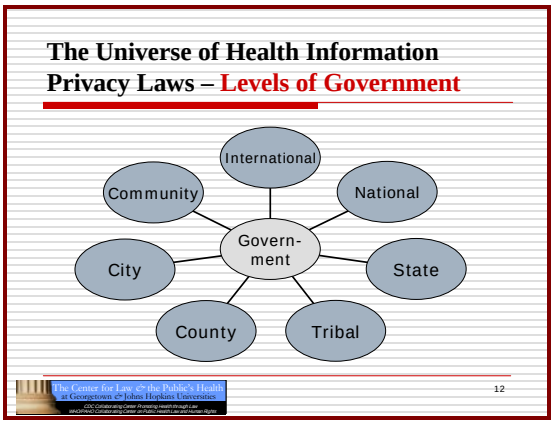
While there are numerous potential risks to health information privacy, these can be neatly summarized into to key points: 1) Accessibility and intimate nature of health data combine to cause social, psychological, and economic harms to those whose privacy is violated; and 2) Emerging computer technologies and the development of longitudinal individual health records and national electronic health information infrastructures are perceived by many to threaten individual privacy. Professor Hodge stressed that the Privacy Rule makes no distinction—any type of health data is viewed as sensitive to individuals. As a result, various infringements or disclosures of that can lead to some significant harms. While emerging computer technologies and the advent of longitudinal individual health records offer interesting new ways to better protect privacy, individuals still often view them as a threat.

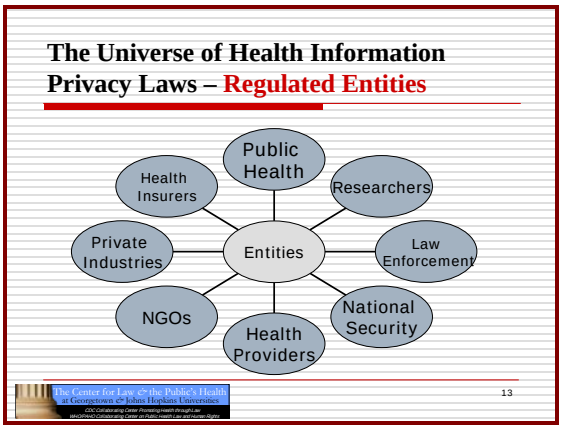
There is an analysis that must be thought through on a different level. This is not just about how to respond to America's fears of privacy, but also people understand that there are synergies in health information privacy. Absent privacy protections, patients and others will

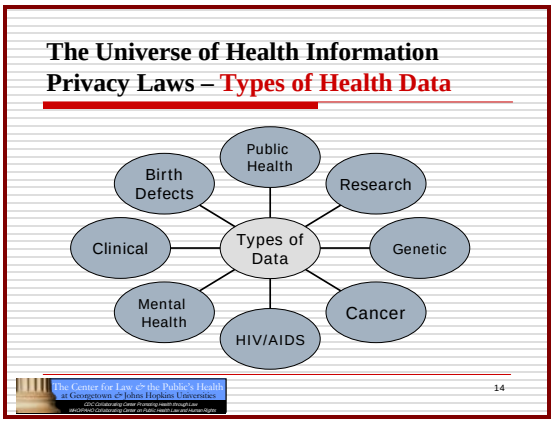
avoid some clinical, public health, and research interventions. However, only through the responsible sharing of some health data may improvements in health care and community health be made. There are synergistic ways in which people can understand that they must be prepared to give up just a little bit of their privacy expectations to allow public health authorities to do what no individual can do alone, which is to protect the public's health. People seem to "get this" increasingly and they understand and are willing to balance various individual interests in privacy with communal interests in conducting health research and public health. Still, individual privacy protections must be balanced with legitimate communal uses of health data like health research and public health. That theme is what underlies many of the privacy laws, specifically the Privacy Rule.

Regarding the universe of health information privacy laws, Professor Hodge stressed that there are a host of laws of every type at every level of government, affecting multiple types of entities, and covering an array of health data are all part of the universe of health information privacy laws:









Every type of law at every jurisdictional level (e.g., treaties, constitutions, statutes, regulations, policies, cases, compacts) all have some implications for how to better protect and regulate the interests of health protection privacy. This is also true at every level of the government (particularly when dealing with massive exchanges of data on an interstate, national, and / or international basis), all of which are implicated and all with the power to implement some sort of privacy protections. These privacy protections affect a variety of entities (e.g., public health, researchers, law enforcement, national security, health providers, et cetera). These laws also cover numerous types of data (e.g., public health, research, genetic, cancer, HIV / AIDS, mental health, clinical, birth defects, et cetera). One important analyses underlying all of this from the universe perspective is if there is a single health record with several of these different types of interests implicated, there may be several different types of privacy laws to which one must be responsive. This is part of what can become problematic with the collection of data.

This is the nature of these privacy laws across the United States. The Privacy Rule will provide some needed clarity. Basic observations underlying all of these laws are that they focus predominately on individual (as contrasted with group) privacy interests; identifiable health data is defined in different ways; the extent of privacy protections varies; and failure to address modern health information exchanges consistent need to balance individual and communal interests in health data. Although an individual is protected, that same individual has virtually no protection as a member of a specific group such as ethnic / minority, religious faction, or family with a certain propensity to cancer. Within many of these protections (particularly at the state level because they are antiquated in many cases) there is a failure to address modern health information. These laws are written as if health records are in the doctors' filing cabinets still, which is not what is happening. Instead, health records are electronic and can be sent across the nation instantly. Hence, many of these laws need significant modification. They still must be prepared to apply some core principles and there remains a consistent need to balance individual / communal interests, which is very evident in the HIPAA Privacy Rule.

Professor Hodge stressed that while people sometimes refer to HIPAA as the "Health Information Privacy Act," he stressed that it is actually "The Health Insurance Portability and Accountability Act of 1996." What does that have to do with health information privacy? Although he stressed that it was a grand oversimplification, Professor Hodge pointed out that HIPAA seeks to do a couple of key things as overriding objectives: *Increase access to health insurance by reducing insurance costs, by lowering administrative costs, by transmitting electronic data under enhanced health information privacy protections that encourage people to seek health care.* A major issue with respect to portability and accountability was that people were leaving one job and then being denied health insurance. In order to increase access to health insurance, the goal was to reduce insurance costs by lowering administrative costs. If electronic data is transmitted like CMS has done for years, claims processing costs are driven down significantly (e.g., savings of billions of dollars). It was recognized that transmitting electronic data would concern Americans, so they would have to do this under enhanced health information privacy protections that encouraged people to seek health care, which is where privacy comes into this act.

HIPAA includes Administrative Simplification Provisions, which required the production of Standards for Privacy of Identifiable Health Information, also known as Health Information Privacy Regulations, located at 45 CFR Parts 160 – 164, and known collectively as the Privacy Rule. Though simplified, the HIPAA timeline basically transpired as follows:

- August, 21, 1996: HIPAA passes Congress and was signed into law.
- August 21, 1999: Congress fails to pass health information privacy law.
- August 1999 - January 2001: Absent Congressional action, DHHS was authorized to produce administrative regulations.
- April 14, 2001: After months of work and public commentary, DHHS finalizes its Privacy Rule with President Bush's approval.
- August 14, 2002: Bush administration modifies original Rule.
- April 14, 2003: The Rule becomes effective for most "covered entities" [or one year later for small health plans].
- April 14, 2004: The Rule is fully effective for all covered entities.

Professor Hodge stressed that he finds consistently (especially with public health partners) that answering the following questions will clarify a great amount of data and interests regarding how to apply the Privacy Rule in this particular setting:

- What is covered?
- Who is covered?
- How is it covered?
- How are disclosures / uses regulated?
- What about other laws?
- What about violations?

"Protected Health Information (PHI)" is what is covered. Simply stated, that is individually-identifiable health information used or disclosed by a covered entity in any form, whether electronically, on paper, or orally. This is very broad. If there is any way whatsoever that the individual in any record can be identified, it is individually identifiable. Even if all of the 18 known identifiers that the HIPAA Privacy Rule uses are stripped and someone can still be identified, it is covered as PHI. However, PHI does not include education records covered by Family Educational Rights and Privacy Act (FERPA); employment records held by a covered entity in its role as employer; or non-identifiable health information. Working with non-identifiable health data is the "out" in terms of the Privacy Rule and the universe of every other privacy law and policy. Non-identifiable data can be collected, acquired, disclosed, stored, and published in the *New York Times,* et cetera. However, this will be extremely stripped down data that will be of minimal utility.

With respect to who is covered, covered entities (CEs) include: Health Plans, Health Care Clearinghouses, Health Providers that exchange identifiable health data electronically, and their business associates. Business associates include: Claims or Data Processors, Billing Companies, Quality Assurance Providers, Utilization Reviewers, Lawyers, Accountants, and Financial Service Providers. Beyond CEs and their Business Associates are those who engage in: 1) Covered functions: those functions of a covered entity the performance of which makes the entity a health plan, health care providers, or health care clearinghouse (45 CFR 164.103); and 2) Hybrid entities performing "covered functions" may have to adhere to relevant portions of the Privacy Rule to the extent to which some part of the entity conducts these activities.

An example of a covered function would be a governmental public health authority setting up a vaccine clinic during the flu season in a Wal-Mart parking lot. There is a minimal $5.00 fee charged and the intent of this vaccine clinic is merely to provide vaccinations to vulnerable people within the population. If the public health authority engages in any type of electronic data transfer, such as providing receipts for insurance coverage or otherwise, this clinic could be considered to be engagement in a covered function, so that public health authority must adhere to the Privacy Rule. There are multiple other examples of how this particular function works. Covered functions definitely complicate the nature of the Privacy Rule and implicate various issues.

Despite all who are covered, not covered are: Life insurances companies; Auto insurance companies; Worker's compensation carriers; Employers not covered unless they are providing group insurance through their employment setting; Others who may still acquire, use, and disclose vast quantities of health data.

There are numerous regulations pertaining to how PHI is covered. The Privacy Rule includes specific boundaries that set limits on uses and disclosures. Security requirements are imposed. Also included are Fair Information Practices, which allow individuals some level of access to their health data (e.g., to amend, inspect, copy, et cetera). Prior to the rule, in some states individuals had no statutory right to access their health data. The Privacy Rule also deals with various issues related to accountability, making covered entities accountable for handling and abuses. In many cases, this includes accounting for disclosures to public health authorities.

There are also distinctions between how uses and disclosures are regulated. *Use* is defined as the sharing, employment, application, utilization, examination, or analysis of PHI within an entity. *Disclosure* is defined as the release, transfer, provision of, access to, or divulging in any other manner of PHI outside the entity holding it. The distinctions are profound even if uses and disclosures are regulated similarly. CEs may use or disclose PHI without individual written authorization to carry out treatment, payment, or health care operations (e.g., standard transactions). Otherwise, uses or disclosures of PHI require either individual opportunities to object or written authorizations pursuant to the "anti-disclosure rule." "Except as otherwise permitted or required. . . , a CE may not use or disclose PHI without an authorization . . . " [45 CFR 164.508(a)(1)]. This is a standard feature of all privacy rules. A neat little trick in the Privacy Rule is that acquisitions equal

disclosures. They are covered very similarly. If someone within an entity is allowed to acquire data, that is viewed as a disclosure. If this is done unlawfully, it will present a problem for both entities involved.

Even with the "anti-disclosure rule" there are exceptions: Law Enforcement, Judicial and Administrative Proceedings, Decedents, Health Emergencies, Limited Commercial Marketing, Minors, Health Research, and Public Health. For example, the Privacy Rule was suspended in the affected regions of Hurricane Katrina for a limited period of time to allow for free-flowing data uses.

Other laws also must be taken into consideration. There are federal and state constitutions, statutory laws, administrative laws, judicial laws, and potentially others. The Privacy Rule does not supplant these laws. The Privacy Rule creates a floor of federal protections. Existing federal or state laws that provide greater health information privacy protections or do not otherwise conflict with the Rule remain in effect. Like a patchwork quilt, they lay over Privacy Rule protections. The analysis of the Privacy Rule itself is not the endpoint—it is the beginning.

Violations or breaches of the Privacy Rule may result in: Complaints filed with the Secretary of DHHS; ensuing investigation by the Secretary; compliance reviews by the Secretary; informal resolution by the Secretary whenever possible; imposition of civil penalties, which can be collected through release of federal debts owed to the entity; and even criminal sanctions against individuals (45 CFR 160.300-.500). While this sounds heavy-handed, these things do not happen. DHHS has used its criminal sanction ability only on a couple of occasions and has not imposed significant civil penalties in any way. These investigations are really designed to bring some sort of formal resolution.

There is another side to enforcement and this side may be where there are more "teeth" to the Privacy Rule than what may occur through a federal office for civil rights. Beyond formal or informal approaches to addressing violations pursuant to the Privacy Rule are: Judicial uses of the Privacy Rule as a *per se* standard for what is expected for protecting health information privacy has been very interesting because there are state claims that can be brought for privacy breeches. If those privacy breeches can be framed as violations of the national standard for protecting privacy set forth in the Privacy Rule, there is more impetus for success on such a complaint. It is a way in which the Privacy Rule is converted to a national standard that can allow for certain types of sanctions. There are contractual obligations as well to adhere to the Privacy Rule. For example, business associates and limited data sets do convey various contractual obligations. If such a contract is breeched, a lawsuit can prevail. Institutional, corporate, and organizational policies that are highly consistent with the Privacy rule require adherence as well. Again, if there are breeches, people may lose their jobs, be sanctioned, et cetera. This is not to say that the Privacy Rule has no real "teeth" to it, but it to say that it is not through the federal government through which those teeth are really implemented.

With regard to the impact of the Privacy Rule on public health, consideration must be given externally to how the Rule impacts the flow of identifiable health data into or out of public

health agencies. Internally, consideration must be given to the ways the Rule affects the practice of public health or public health research conducted by public health agencies or its partners. The external issues are probably the most profound for public health because the types and places that CDC or state partners may want to go to obtain these data for a public health surveillance system are very likely going to be covered entities. Hence, consideration also must be given to what the covered entities' ability to deny data or restrict data flow.

While there are many exceptions to the Privacy Rule, it does contain what is known as the "Public Health" Exception. The "public health" exception to the anti-disclosure rule states that a covered entity may disclose PHI without specific, individual authorization to a "*public health authority* that is authorized by law to collect and receive such information for the purpose of preventing and controlling disease, injury, or disability, including . . . reporting of disease . . . and the conduct of public health surveillance . . . " Basically this clause says, "Covered entities are not in their right mind to deny access to these data for public health surveillance purposes to public health authorities. They have a legitimate right to these data. It is part of the balance of what we are attempting to do with the Privacy Rule. Give it to them if they ask for it and they have some claim to it pursuant to some authorization of law that does not have to be specific to the actually type of surveillance. It is just a generalized claim that is intended to do exactly that."

Beyond this general authorization, additional, specific public health-based exceptions include:

- ❑ Disclosures to maintain the quality, safety, or effectiveness of FDA products
- ❑ Disclosures to notify persons exposed to communicable diseases
- ❑ Disclosures concerning work-related injuries
- ❑ Disclosures about victims of abuse, neglect, or domestic violence
- ❑ Disclosures for health oversight activities
- ❑ Disclosures to prevent serious threats to persons or the public

A "public health authority" is defined as an "agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency . . . that is responsible for public health matters as part of its official mandate." Public health authorities under this type of rule include: CDC, FDA, NIH, State or Tribal Health Departments, Local Health Departments, Contractors / Others acting under authority of these agencies. A private sector entity collecting data under a granted authority from any level of governmental public health agency is viewed as a public health authority under this act. Professor Hodge highlighted this component, given that it is not well understood.

In terms of state public health reporting laws, the Privacy Rule does not pre-empt (or override) state law that "provides for the reporting of disease or injury . . . or for the conduct of public health surveillance [or] investigation . . . ." The Privacy Rule has nothing to say about state public health reporting laws because it is a privacy act. It does not restrict, allow

instead was to focus on how public health could carry out its work consistent with privacy rules. He also stressed that while he would focus on the Privacy Rule, there was a host of additional privacy laws in various jurisdictions of which they must be cognizant and compliant. Participants were referred to two articles in their packets summarizing the privacy laws outside the Privacy Rule, as well as the Center for Disease Control and Prevention's (CDC's) cleared guidance pertaining to the impact of the Privacy Rule on public health authorities.

With respect to key legal terms, although they are often used interchangeably, there are distinctions between *Privacy*, *Confidentiality*, and *Security*: 1) Privacy is an individual's right to control their identifiable health information in the broadest perspective; 2) Confidentiality concerns privacy interests that arise from a specific relationship (e.g., doctor / patient, researcher / subject) and corresponding legal and ethical duties; and 3) Security regards technological or administrative safeguards or tools to protect identifiable health information from unwarranted access, use, or disclosure. Professor Hodge shared the following quote from Willis Ware because it offers a good way to frame these various perspectives accurately: "If the security safeguards in an automated system fail or are compromised, a breach of confidentiality can occur and the privacy of data subjects invaded."

Most people appropriately think first about what can be done to restrict disclosures. While this is a core concept of privacy, it is not the only one. They must also be cognizant of three other major factors that are built into the Privacy Rule as well as a lot of the privacy laws. It is not just about how records are properly disclosed, but also is about how they are acquired, used, and stored. Privacy violations and infringements can come from unlawful acquisitions of data. If data is acquired for an ALS surveillance system, but is then used for purposes completely unrelated to surveillance of that disease across the nation, this constitutes a privacy violation. The data may be acquired lawfully, used in the manner intended, and not disclosed in any inappropriate way. However, if it is stored in a haphazard fashion on a laptop that is stolen from someone's trunk, there is now a storage related issue, a security concern, and a privacy violation.

While there are numerous potential risks to health information privacy, these can be neatly summarized into to key points: 1) Accessibility and intimate nature of health data combine to cause social, psychological, and economic harms to those whose privacy is violated; and 2) Emerging computer technologies and the development of longitudinal individual health records and national electronic health information infrastructures are perceived by many to threaten individual privacy. Professor Hodge stressed that the Privacy Rule makes no distinction—any type of health data is viewed as sensitive to individuals. As a result, various infringements or disclosures of that can lead to some significant harms. While emerging computer technologies and the advent of longitudinal individual health records offer interesting new ways to better protect privacy, individuals still often view them as a threat.

There is an analysis that must be thought through on a different level. This is not just about how to respond to America's fears of privacy, but also people understand that there are synergies in health information privacy. Absent privacy protections, patients and others will

HIPAA includes Administrative Simplification Provisions, which required the production of Standards for Privacy of Identifiable Health Information, also known as Health Information Privacy Regulations, located at 45 CFR Parts 160 – 164, and known collectively as the Privacy Rule. Though simplified, the HIPAA timeline basically transpired as follows:

- August, 21, 1996: HIPAA passes Congress and was signed into law.
- August 21, 1999: Congress fails to pass health information privacy law.
- August 1999 - January 2001: Absent Congressional action, DHHS was authorized to produce administrative regulations.
- April 14, 2001: After months of work and public commentary, DHHS finalizes its Privacy Rule with President Bush's approval.
- August 14, 2002: Bush administration modifies original Rule.
- April 14, 2003: The Rule becomes effective for most "covered entities" [or one year later for small health plans].
- April 14, 2004: The Rule is fully effective for all covered entities.

Professor Hodge stressed that he finds consistently (especially with public health partners) that answering the following questions will clarify a great amount of data and interests regarding how to apply the Privacy Rule in this particular setting:

- What is covered?
- Who is covered?
- How is it covered?
- How are disclosures / uses regulated?
- What about other laws?
- What about violations?

"Protected Health Information (PHI)" is what is covered. Simply stated, that is individually-identifiable health information used or disclosed by a covered entity in any form, whether electronically, on paper, or orally. This is very broad. If there is any way whatsoever that the individual in any record can be identified, it is individually identifiable. Even if all of the 18 known identifiers that the HIPAA Privacy Rule uses are stripped and someone can still be identified, it is covered as PHI. However, PHI does not include education records covered by Family Educational Rights and Privacy Act (FERPA); employment records held by a covered entity in its role as employer; or non-identifiable health information. Working with non-identifiable health data is the "out" in terms of the Privacy Rule and the universe of every other privacy law and policy. Non-identifiable data can be collected, acquired, disclosed, stored, and published in the *New York Times,* et cetera. However, this will be extremely stripped down data that will be of minimal utility.

With respect to who is covered, covered entities (CEs) include: Health Plans, Health Care Clearinghouses, Health Providers that exchange identifiable health data electronically, and their business associates. Business associates include: Claims or Data Processors, Billing Companies, Quality Assurance Providers, Utilization Reviewers, Lawyers, Accountants, and Financial Service Providers. Beyond CEs and their Business Associates are those who engage in: 1) Covered functions: those functions of a covered entity the performance of which makes the entity a health plan, health care providers, or health care clearinghouse (45 CFR 164.103); and 2) Hybrid entities performing "covered functions" may have to adhere to relevant portions of the Privacy Rule to the extent to which some part of the entity conducts these activities.

An example of a covered function would be a governmental public health authority setting up a vaccine clinic during the flu season in a Wal-Mart parking lot. There is a minimal $5.00 fee charged and the intent of this vaccine clinic is merely to provide vaccinations to vulnerable people within the population. If the public health authority engages in any type of electronic data transfer, such as providing receipts for insurance coverage or otherwise, this clinic could be considered to be engagement in a covered function, so that public health authority must adhere to the Privacy Rule. There are multiple other examples of how this particular function works. Covered functions definitely complicate the nature of the Privacy Rule and implicate various issues.

Despite all who are covered, not covered are: Life insurances companies; Auto insurance companies; Worker's compensation carriers; Employers not covered unless they are providing group insurance through their employment setting; Others who may still acquire, use, and disclose vast quantities of health data.

There are numerous regulations pertaining to how PHI is covered. The Privacy Rule includes specific boundaries that set limits on uses and disclosures. Security requirements are imposed. Also included are Fair Information Practices, which allow individuals some level of access to their health data (e.g., to amend, inspect, copy, et cetera). Prior to the rule, in some states individuals had no statutory right to access their health data. The Privacy Rule also deals with various issues related to accountability, making covered entities accountable for handling and abuses. In many cases, this includes accounting for disclosures to public health authorities.

There are also distinctions between how uses and disclosures are regulated. *Use* is defined as the sharing, employment, application, utilization, examination, or analysis of PHI within an entity. *Disclosure* is defined as the release, transfer, provision of, access to, or divulging in any other manner of PHI outside the entity holding it. The distinctions are profound even if uses and disclosures are regulated similarly. CEs may use or disclose PHI without individual written authorization to carry out treatment, payment, or health care operations (e.g., standard transactions). Otherwise, uses or disclosures of PHI require either individual opportunities to object or written authorizations pursuant to the "anti-disclosure rule." "Except as otherwise permitted or required. . . , a CE may not use or disclose PHI without an authorization . . . " [45 CFR 164.508(a)(1)]. This is a standard feature of all privacy rules. A neat little trick in the Privacy Rule is that acquisitions equal

disclosures. They are covered very similarly. If someone within an entity is allowed to acquire data, that is viewed as a disclosure. If this is done unlawfully, it will present a problem for both entities involved.

Even with the "anti-disclosure rule" there are exceptions: Law Enforcement, Judicial and Administrative Proceedings, Decedents, Health Emergencies, Limited Commercial Marketing, Minors, Health Research, and Public Health. For example, the Privacy Rule was suspended in the affected regions of Hurricane Katrina for a limited period of time to allow for free-flowing data uses.

Other laws also must be taken into consideration. There are federal and state constitutions, statutory laws, administrative laws, judicial laws, and potentially others. The Privacy Rule does not supplant these laws. The Privacy Rule creates a floor of federal protections. Existing federal or state laws that provide greater health information privacy protections or do not otherwise conflict with the Rule remain in effect. Like a patchwork quilt, they lay over Privacy Rule protections. The analysis of the Privacy Rule itself is not the endpoint—it is the beginning.

Violations or breaches of the Privacy Rule may result in: Complaints filed with the Secretary of DHHS; ensuing investigation by the Secretary; compliance reviews by the Secretary; informal resolution by the Secretary whenever possible; imposition of civil penalties, which can be collected through release of federal debts owed to the entity; and even criminal sanctions against individuals (45 CFR 160.300-.500). While this sounds heavy-handed, these things do not happen. DHHS has used its criminal sanction ability only on a couple of occasions and has not imposed significant civil penalties in any way. These investigations are really designed to bring some sort of formal resolution.

There is another side to enforcement and this side may be where there are more "teeth" to the Privacy Rule than what may occur through a federal office for civil rights. Beyond formal or informal approaches to addressing violations pursuant to the Privacy Rule are: Judicial uses of the Privacy Rule as a *per se* standard for what is expected for protecting health information privacy has been very interesting because there are state claims that can be brought for privacy breeches. If those privacy breeches can be framed as violations of the national standard for protecting privacy set forth in the Privacy Rule, there is more impetus for success on such a complaint. It is a way in which the Privacy Rule is converted to a national standard that can allow for certain types of sanctions. There are contractual obligations as well to adhere to the Privacy Rule. For example, business associates and limited data sets do convey various contractual obligations. If such a contract is breeched, a lawsuit can prevail. Institutional, corporate, and organizational policies that are highly consistent with the Privacy rule require adherence as well. Again, if there are breeches, people may lose their jobs, be sanctioned, et cetera. This is not to say that the Privacy Rule has no real "teeth" to it, but it to say that it is not through the federal government through which those teeth are really implemented.

With regard to the impact of the Privacy Rule on public health, consideration must be given externally to how the Rule impacts the flow of identifiable health data into or out of public

health agencies. Internally, consideration must be given to the ways the Rule affects the practice of public health or public health research conducted by public health agencies or its partners. The external issues are probably the most profound for public health because the types and places that CDC or state partners may want to go to obtain these data for a public health surveillance system are very likely going to be covered entities. Hence, consideration also must be given to what the covered entities' ability to deny data or restrict data flow.

While there are many exceptions to the Privacy Rule, it does contain what is known as the "Public Health" Exception. The "public health" exception to the anti-disclosure rule states that a covered entity may disclose PHI without specific, individual authorization to a "*public health authority* that is authorized by law to collect and receive such information for the purpose of preventing and controlling disease, injury, or disability, including . . . reporting of disease . . . and the conduct of public health surveillance . . . " Basically this clause says, "Covered entities are not in their right mind to deny access to these data for public health surveillance purposes to public health authorities. They have a legitimate right to these data. It is part of the balance of what we are attempting to do with the Privacy Rule. Give it to them if they ask for it and they have some claim to it pursuant to some authorization of law that does not have to be specific to the actually type of surveillance. It is just a generalized claim that is intended to do exactly that."

Beyond this general authorization, additional, specific public health-based exceptions include:

- ❑ Disclosures to maintain the quality, safety, or effectiveness of FDA products
- ❑ Disclosures to notify persons exposed to communicable diseases
- ❑ Disclosures concerning work-related injuries
- ❑ Disclosures about victims of abuse, neglect, or domestic violence
- ❑ Disclosures for health oversight activities
- ❑ Disclosures to prevent serious threats to persons or the public

A "public health authority" is defined as an "agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency . . . that is responsible for public health matters as part of its official mandate." Public health authorities under this type of rule include: CDC, FDA, NIH, State or Tribal Health Departments, Local Health Departments, Contractors / Others acting under authority of these agencies. A private sector entity collecting data under a granted authority from any level of governmental public health agency is viewed as a public health authority under this act. Professor Hodge highlighted this component, given that it is not well understood.

In terms of state public health reporting laws, the Privacy Rule does not pre-empt (or override) state law that "provides for the reporting of disease or injury . . . or for the conduct of public health surveillance [or] investigation . . . ." The Privacy Rule has nothing to say about state public health reporting laws because it is a privacy act. It does not restrict, allow

for, or require different data disclosures. It simply regulates the privacy between exchanges. Existing state reporting laws are, therefore, still full and effective.

Regarding the impact of the Privacy Rule on public health internally, an essential message that is beneficial to know is that, to the extent that public health authorities use or disclose identifiable health data for public health purposes, they are not "covered entities," and are thus not required to adhere to the provisions of the Privacy Rule. Simply stated, public health authorities doing public health things are not covered by the Rule. The Rule has nothing to say about what public health entities do with data internally until those public health authorities start to act like, look like, or do things that approximate what a health provider or health insurance plan might do. That is, a profound area of potential impact concerns the activities of public health authorities that resemble the provision of health care (e.g., direct delivery of health services to disadvantaged individuals) or administration of health plans (e.g., state "well person" programs). Public health authorities performing health care activities or acting as a health plan are engaged in "covered functions," and accordingly must adhere to the Privacy Rule.

Most public health authorities at the state and local levels declare themselves as hybrid entities (or multi-functional organizations with covered entity components) pursuant to the Rule. Johns Hopkins, for example, has elected hybrid status. This allows their hospital to be viewed as a covered entity, but does not require the School of Engineering to be viewed as such. Absent the election of hybrid status, an entire enterprise is viewed as covered by the privacy rule. For state health departments that have only a component of what they do considered to be a health provider type function, electing hybrid status would make only that part of the entity be required to adhere to the Rule. Simply stated, the practical effect of hybrid status is that the public health agency designates those components of its practices that are covered, and adheres to the Rule concerning those components. Others within the agency may not have to adhere to the same requirements concerning their duties, although the agency is responsible for their compliance with covered applications.

In terms of distinguishing public health practice versus research, the HIPAA Privacy Rule provides different standards for disclosing PHI without authorization for public health versus research purposes. Professor Hodge stressed that he is working with federal, state, and local officials and others to help simplify the distinctions. As well, the Office for Human Research Protections (OHRP) will soon release new guidance that may also help draw distinctions between public health practice and research.

Part of the impetus for clear distinctions relates to the fact that the HIPAA Privacy Rule standards for providing data without authorization for public health purposes are much broader than those concerning disclosures for research purposes. Disclosures for research purposes are more restrictive. Absent some narrow exceptions, research disclosures require IRB or Privacy Board agreement that the use or disclosure of PHI involves no more than a minimal risk to individual privacy based on an adequate plan to protect the identifiers from improper use and disclosure; an adequate plan to destroy identifiers as soon as possible; and adequate written assurances that PHI will not be reused or disclosed to anyone else except as required by law. There are other provisions as well. Some access to

data may be allowed without written authorization for preparation to research, for research on decedents, and for limited data sets (e.g., basically stripped down of all of the 18 HIPAA identifiers—virtually useless to many public health authorities).

The key issue is that neither the HIPAA Privacy Rule nor the federal Common Rule (regulating the performance or funding of human subjects research by most federal agencies) clearly distinguishes public health practice activities from research activities. Multiple dilemmas arise as a result: Public health practice activities that assimilate research activities, such as some types of surveillance, may be seriously misconstrued; Covered entities may deny access to PHI to public health authorities on the grounds that the requested basis for the data is research, and not practice. Public health practice activities may ultimately be submitted for IRB approval as if they are research. Public health practitioners do not have the money or the time to be seeking IRB approval for routine, public health activities.

Professor Hodge briefly walked participants through the publication titled, "A Report for Public Health Practitioners Including Case Studies and Guidance for Making Distinctions." This guidance was sponsored by the Council for State and Territorial Epidemiologists (CSTE) and is available in full on the CSTE website. The principle objectives of the guidance are to: assess legal and ethical environments underlying public health practice and human subject research; clarify existing definitions of public health practice and research; provide meaningful cases on practice and research; and make distinctions between public health practice and research through foundational and enhanced guidance. Professor Hodge stressed that this is of great importance to ALS / MS surveillance systems because of what they may be doing with the data. If the next step to acquiring the data is to engage in systematic research using the data, this could have implications with respect to the various entities being willing to provide the data.

The guidance provides functional definitions where there are none. "Public health practice" is defined as the collection and analysis of identifiable health data by a public health authority for the purpose of protecting the health of a particular community, where the benefits and risks are primarily designed to accrue to the participating community. This definition relate to the context of public health authorities attempting to acquire large amounts of identifiable health data through covered entities. It is the collection and analyses of those data by public health authorities for the purpose of protecting the health of a particular community, where the benefits or risks are primarily designed to accrue to that participating community. In contrast, "public health research" is defined as the systematic collection and analysis of identifiable health data by a public health authority for the purpose of generating knowledge that will primarily benefit those beyond the participating community who bear the risks of participation.

This publication includes a checklist that offers a way to make simple and then more difficult distinctions between practice versus research in an effort to bring some consistency to the approach. This checklist was built by noting that there are some core essential features of foundations of practice versus research that are very different. If these are assessed through the checklist, one can quickly distinguish many cases. For the more difficult cases,

HIPAA includes Administrative Simplification Provisions, which required the production of Standards for Privacy of Identifiable Health Information, also known as Health Information Privacy Regulations, located at 45 CFR Parts 160 – 164, and known collectively as the Privacy Rule. Though simplified, the HIPAA timeline basically transpired as follows:

- August, 21, 1996: HIPAA passes Congress and was signed into law.
- August 21, 1999: Congress fails to pass health information privacy law.
- August 1999 - January 2001: Absent Congressional action, DHHS was authorized to produce administrative regulations.
- April 14, 2001: After months of work and public commentary, DHHS finalizes its Privacy Rule with President Bush's approval.
- August 14, 2002: Bush administration modifies original Rule.
- April 14, 2003: The Rule becomes effective for most "covered entities" [or one year later for small health plans].
- April 14, 2004: The Rule is fully effective for all covered entities.

Professor Hodge stressed that he finds consistently (especially with public health partners) that answering the following questions will clarify a great amount of data and interests regarding how to apply the Privacy Rule in this particular setting:

- What is covered?
- Who is covered?
- How is it covered?
- How are disclosures / uses regulated?
- What about other laws?
- What about violations?

"Protected Health Information (PHI)" is what is covered. Simply stated, that is individually-identifiable health information used or disclosed by a covered entity in any form, whether electronically, on paper, or orally. This is very broad. If there is any way whatsoever that the individual in any record can be identified, it is individually identifiable. Even if all of the 18 known identifiers that the HIPAA Privacy Rule uses are stripped and someone can still be identified, it is covered as PHI. However, PHI does not include education records covered by Family Educational Rights and Privacy Act (FERPA); employment records held by a covered entity in its role as employer; or non-identifiable health information. Working with non-identifiable health data is the "out" in terms of the Privacy Rule and the universe of every other privacy law and policy. Non-identifiable data can be collected, acquired, disclosed, stored, and published in the *New York Times,* et cetera. However, this will be extremely stripped down data that will be of minimal utility.

With respect to who is covered, covered entities (CEs) include: Health Plans, Health Care Clearinghouses, Health Providers that exchange identifiable health data electronically, and their business associates. Business associates include: Claims or Data Processors, Billing Companies, Quality Assurance Providers, Utilization Reviewers, Lawyers, Accountants, and Financial Service Providers. Beyond CEs and their Business Associates are those who engage in: 1) Covered functions: those functions of a covered entity the performance of which makes the entity a health plan, health care providers, or health care clearinghouse (45 CFR 164.103); and 2) Hybrid entities performing "covered functions" may have to adhere to relevant portions of the Privacy Rule to the extent to which some part of the entity conducts these activities.

An example of a covered function would be a governmental public health authority setting up a vaccine clinic during the flu season in a Wal-Mart parking lot. There is a minimal $5.00 fee charged and the intent of this vaccine clinic is merely to provide vaccinations to vulnerable people within the population. If the public health authority engages in any type of electronic data transfer, such as providing receipts for insurance coverage or otherwise, this clinic could be considered to be engagement in a covered function, so that public health authority must adhere to the Privacy Rule. There are multiple other examples of how this particular function works. Covered functions definitely complicate the nature of the Privacy Rule and implicate various issues.

Despite all who are covered, not covered are: Life insurances companies; Auto insurance companies; Worker's compensation carriers; Employers not covered unless they are providing group insurance through their employment setting; Others who may still acquire, use, and disclose vast quantities of health data.

There are numerous regulations pertaining to how PHI is covered. The Privacy Rule includes specific boundaries that set limits on uses and disclosures. Security requirements are imposed. Also included are Fair Information Practices, which allow individuals some level of access to their health data (e.g., to amend, inspect, copy, et cetera). Prior to the rule, in some states individuals had no statutory right to access their health data. The Privacy Rule also deals with various issues related to accountability, making covered entities accountable for handling and abuses. In many cases, this includes accounting for disclosures to public health authorities.

There are also distinctions between how uses and disclosures are regulated. *Use* is defined as the sharing, employment, application, utilization, examination, or analysis of PHI within an entity. *Disclosure* is defined as the release, transfer, provision of, access to, or divulging in any other manner of PHI outside the entity holding it. The distinctions are profound even if uses and disclosures are regulated similarly. CEs may use or disclose PHI without individual written authorization to carry out treatment, payment, or health care operations (e.g., standard transactions). Otherwise, uses or disclosures of PHI require either individual opportunities to object or written authorizations pursuant to the "anti-disclosure rule." "Except as otherwise permitted or required. . . , a CE may not use or disclose PHI without an authorization . . . " [45 CFR 164.508(a)(1)]. This is a standard feature of all privacy rules. A neat little trick in the Privacy Rule is that acquisitions equal

disclosures. They are covered very similarly. If someone within an entity is allowed to acquire data, that is viewed as a disclosure. If this is done unlawfully, it will present a problem for both entities involved.

Even with the "anti-disclosure rule" there are exceptions: Law Enforcement, Judicial and Administrative Proceedings, Decedents, Health Emergencies, Limited Commercial Marketing, Minors, Health Research, and Public Health. For example, the Privacy Rule was suspended in the affected regions of Hurricane Katrina for a limited period of time to allow for free-flowing data uses.

Other laws also must be taken into consideration. There are federal and state constitutions, statutory laws, administrative laws, judicial laws, and potentially others. The Privacy Rule does not supplant these laws. The Privacy Rule creates a floor of federal protections. Existing federal or state laws that provide greater health information privacy protections or do not otherwise conflict with the Rule remain in effect. Like a patchwork quilt, they lay over Privacy Rule protections. The analysis of the Privacy Rule itself is not the endpoint—it is the beginning.

Violations or breaches of the Privacy Rule may result in: Complaints filed with the Secretary of DHHS; ensuing investigation by the Secretary; compliance reviews by the Secretary; informal resolution by the Secretary whenever possible; imposition of civil penalties, which can be collected through release of federal debts owed to the entity; and even criminal sanctions against individuals (45 CFR 160.300-.500). While this sounds heavy-handed, these things do not happen. DHHS has used its criminal sanction ability only on a couple of occasions and has not imposed significant civil penalties in any way. These investigations are really designed to bring some sort of formal resolution.

There is another side to enforcement and this side may be where there are more "teeth" to the Privacy Rule than what may occur through a federal office for civil rights. Beyond formal or informal approaches to addressing violations pursuant to the Privacy Rule are: Judicial uses of the Privacy Rule as a *per se* standard for what is expected for protecting health information privacy has been very interesting because there are state claims that can be brought for privacy breeches. If those privacy breeches can be framed as violations of the national standard for protecting privacy set forth in the Privacy Rule, there is more impetus for success on such a complaint. It is a way in which the Privacy Rule is converted to a national standard that can allow for certain types of sanctions. There are contractual obligations as well to adhere to the Privacy Rule. For example, business associates and limited data sets do convey various contractual obligations. If such a contract is breeched, a lawsuit can prevail. Institutional, corporate, and organizational policies that are highly consistent with the Privacy rule require adherence as well. Again, if there are breeches, people may lose their jobs, be sanctioned, et cetera. This is not to say that the Privacy Rule has no real "teeth" to it, but it to say that it is not through the federal government through which those teeth are really implemented.

With regard to the impact of the Privacy Rule on public health, consideration must be given externally to how the Rule impacts the flow of identifiable health data into or out of public

health agencies. Internally, consideration must be given to the ways the Rule affects the practice of public health or public health research conducted by public health agencies or its partners. The external issues are probably the most profound for public health because the types and places that CDC or state partners may want to go to obtain these data for a public health surveillance system are very likely going to be covered entities. Hence, consideration also must be given to what the covered entities' ability to deny data or restrict data flow.

While there are many exceptions to the Privacy Rule, it does contain what is known as the "Public Health" Exception. The "public health" exception to the anti-disclosure rule states that a covered entity may disclose PHI without specific, individual authorization to a "*public health authority* that is authorized by law to collect and receive such information for the purpose of preventing and controlling disease, injury, or disability, including . . . reporting of disease . . . and the conduct of public health surveillance . . . " Basically this clause says, "Covered entities are not in their right mind to deny access to these data for public health surveillance purposes to public health authorities. They have a legitimate right to these data. It is part of the balance of what we are attempting to do with the Privacy Rule. Give it to them if they ask for it and they have some claim to it pursuant to some authorization of law that does not have to be specific to the actually type of surveillance. It is just a generalized claim that is intended to do exactly that."

Beyond this general authorization, additional, specific public health-based exceptions include:

- ❑ Disclosures to maintain the quality, safety, or effectiveness of FDA products
- ❑ Disclosures to notify persons exposed to communicable diseases
- ❑ Disclosures concerning work-related injuries
- ❑ Disclosures about victims of abuse, neglect, or domestic violence
- ❑ Disclosures for health oversight activities
- ❑ Disclosures to prevent serious threats to persons or the public

A "public health authority" is defined as an "agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency . . . that is responsible for public health matters as part of its official mandate." Public health authorities under this type of rule include: CDC, FDA, NIH, State or Tribal Health Departments, Local Health Departments, Contractors / Others acting under authority of these agencies. A private sector entity collecting data under a granted authority from any level of governmental public health agency is viewed as a public health authority under this act. Professor Hodge highlighted this component, given that it is not well understood.

In terms of state public health reporting laws, the Privacy Rule does not pre-empt (or override) state law that "provides for the reporting of disease or injury . . . or for the conduct of public health surveillance [or] investigation . . . ." The Privacy Rule has nothing to say about state public health reporting laws because it is a privacy act. It does not restrict, allow

instead was to focus on how public health could carry out its work consistent with privacy rules. He also stressed that while he would focus on the Privacy Rule, there was a host of additional privacy laws in various jurisdictions of which they must be cognizant and compliant. Participants were referred to two articles in their packets summarizing the privacy laws outside the Privacy Rule, as well as the Center for Disease Control and Prevention's (CDC's) cleared guidance pertaining to the impact of the Privacy Rule on public health authorities.

With respect to key legal terms, although they are often used interchangeably, there are distinctions between *Privacy*, *Confidentiality*, and *Security*: 1) Privacy is an individual's right to control their identifiable health information in the broadest perspective; 2) Confidentiality concerns privacy interests that arise from a specific relationship (e.g., doctor / patient, researcher / subject) and corresponding legal and ethical duties; and 3) Security regards technological or administrative safeguards or tools to protect identifiable health information from unwarranted access, use, or disclosure. Professor Hodge shared the following quote from Willis Ware because it offers a good way to frame these various perspectives accurately: "If the security safeguards in an automated system fail or are compromised, a breach of confidentiality can occur and the privacy of data subjects invaded."

Most people appropriately think first about what can be done to restrict disclosures. While this is a core concept of privacy, it is not the only one. They must also be cognizant of three other major factors that are built into the Privacy Rule as well as a lot of the privacy laws. It is not just about how records are properly disclosed, but also is about how they are acquired, used, and stored. Privacy violations and infringements can come from unlawful acquisitions of data. If data is acquired for an ALS surveillance system, but is then used for purposes completely unrelated to surveillance of that disease across the nation, this constitutes a privacy violation. The data may be acquired lawfully, used in the manner intended, and not disclosed in any inappropriate way. However, if it is stored in a haphazard fashion on a laptop that is stolen from someone's trunk, there is now a storage related issue, a security concern, and a privacy violation.

While there are numerous potential risks to health information privacy, these can be neatly summarized into to key points: 1) Accessibility and intimate nature of health data combine to cause social, psychological, and economic harms to those whose privacy is violated; and 2) Emerging computer technologies and the development of longitudinal individual health records and national electronic health information infrastructures are perceived by many to threaten individual privacy. Professor Hodge stressed that the Privacy Rule makes no distinction—any type of health data is viewed as sensitive to individuals. As a result, various infringements or disclosures of that can lead to some significant harms. While emerging computer technologies and the advent of longitudinal individual health records offer interesting new ways to better protect privacy, individuals still often view them as a threat.

There is an analysis that must be thought through on a different level. This is not just about how to respond to America's fears of privacy, but also people understand that there are synergies in health information privacy. Absent privacy protections, patients and others will

HIPAA includes Administrative Simplification Provisions, which required the production of Standards for Privacy of Identifiable Health Information, also known as Health Information Privacy Regulations, located at 45 CFR Parts 160 – 164, and known collectively as the Privacy Rule. Though simplified, the HIPAA timeline basically transpired as follows:

- August, 21, 1996: HIPAA passes Congress and was signed into law.
- August 21, 1999: Congress fails to pass health information privacy law.
- August 1999 - January 2001: Absent Congressional action, DHHS was authorized to produce administrative regulations.
- April 14, 2001: After months of work and public commentary, DHHS finalizes its Privacy Rule with President Bush's approval.
- August 14, 2002: Bush administration modifies original Rule.
- April 14, 2003: The Rule becomes effective for most "covered entities" [or one year later for small health plans].
- April 14, 2004: The Rule is fully effective for all covered entities.

Professor Hodge stressed that he finds consistently (especially with public health partners) that answering the following questions will clarify a great amount of data and interests regarding how to apply the Privacy Rule in this particular setting:

- What is covered?
- Who is covered?
- How is it covered?
- How are disclosures / uses regulated?
- What about other laws?
- What about violations?

"Protected Health Information (PHI)" is what is covered. Simply stated, that is individually-identifiable health information used or disclosed by a covered entity in any form, whether electronically, on paper, or orally. This is very broad. If there is any way whatsoever that the individual in any record can be identified, it is individually identifiable. Even if all of the 18 known identifiers that the HIPAA Privacy Rule uses are stripped and someone can still be identified, it is covered as PHI. However, PHI does not include education records covered by Family Educational Rights and Privacy Act (FERPA); employment records held by a covered entity in its role as employer; or non-identifiable health information. Working with non-identifiable health data is the "out" in terms of the Privacy Rule and the universe of every other privacy law and policy. Non-identifiable data can be collected, acquired, disclosed, stored, and published in the *New York Times,* et cetera. However, this will be extremely stripped down data that will be of minimal utility.

With respect to who is covered, covered entities (CEs) include: Health Plans, Health Care Clearinghouses, Health Providers that exchange identifiable health data electronically, and their business associates. Business associates include: Claims or Data Processors, Billing Companies, Quality Assurance Providers, Utilization Reviewers, Lawyers, Accountants, and Financial Service Providers. Beyond CEs and their Business Associates are those who engage in: 1) Covered functions: those functions of a covered entity the performance of which makes the entity a health plan, health care providers, or health care clearinghouse (45 CFR 164.103); and 2) Hybrid entities performing "covered functions" may have to adhere to relevant portions of the Privacy Rule to the extent to which some part of the entity conducts these activities.

An example of a covered function would be a governmental public health authority setting up a vaccine clinic during the flu season in a Wal-Mart parking lot. There is a minimal $5.00 fee charged and the intent of this vaccine clinic is merely to provide vaccinations to vulnerable people within the population. If the public health authority engages in any type of electronic data transfer, such as providing receipts for insurance coverage or otherwise, this clinic could be considered to be engagement in a covered function, so that public health authority must adhere to the Privacy Rule. There are multiple other examples of how this particular function works. Covered functions definitely complicate the nature of the Privacy Rule and implicate various issues.

Despite all who are covered, not covered are: Life insurances companies; Auto insurance companies; Worker's compensation carriers; Employers not covered unless they are providing group insurance through their employment setting; Others who may still acquire, use, and disclose vast quantities of health data.

There are numerous regulations pertaining to how PHI is covered. The Privacy Rule includes specific boundaries that set limits on uses and disclosures. Security requirements are imposed. Also included are Fair Information Practices, which allow individuals some level of access to their health data (e.g., to amend, inspect, copy, et cetera). Prior to the rule, in some states individuals had no statutory right to access their health data. The Privacy Rule also deals with various issues related to accountability, making covered entities accountable for handling and abuses. In many cases, this includes accounting for disclosures to public health authorities.

There are also distinctions between how uses and disclosures are regulated. *Use* is defined as the sharing, employment, application, utilization, examination, or analysis of PHI within an entity. *Disclosure* is defined as the release, transfer, provision of, access to, or divulging in any other manner of PHI outside the entity holding it. The distinctions are profound even if uses and disclosures are regulated similarly. CEs may use or disclose PHI without individual written authorization to carry out treatment, payment, or health care operations (e.g., standard transactions). Otherwise, uses or disclosures of PHI require either individual opportunities to object or written authorizations pursuant to the "anti-disclosure rule." "Except as otherwise permitted or required. . . , a CE may not use or disclose PHI without an authorization . . . " [45 CFR 164.508(a)(1)]. This is a standard feature of all privacy rules. A neat little trick in the Privacy Rule is that acquisitions equal

disclosures. They are covered very similarly. If someone within an entity is allowed to acquire data, that is viewed as a disclosure. If this is done unlawfully, it will present a problem for both entities involved.

Even with the "anti-disclosure rule" there are exceptions: Law Enforcement, Judicial and Administrative Proceedings, Decedents, Health Emergencies, Limited Commercial Marketing, Minors, Health Research, and Public Health. For example, the Privacy Rule was suspended in the affected regions of Hurricane Katrina for a limited period of time to allow for free-flowing data uses.

Other laws also must be taken into consideration. There are federal and state constitutions, statutory laws, administrative laws, judicial laws, and potentially others. The Privacy Rule does not supplant these laws. The Privacy Rule creates a floor of federal protections. Existing federal or state laws that provide greater health information privacy protections or do not otherwise conflict with the Rule remain in effect. Like a patchwork quilt, they lay over Privacy Rule protections. The analysis of the Privacy Rule itself is not the endpoint—it is the beginning.

Violations or breaches of the Privacy Rule may result in: Complaints filed with the Secretary of DHHS; ensuing investigation by the Secretary; compliance reviews by the Secretary; informal resolution by the Secretary whenever possible; imposition of civil penalties, which can be collected through release of federal debts owed to the entity; and even criminal sanctions against individuals (45 CFR 160.300-.500). While this sounds heavy-handed, these things do not happen. DHHS has used its criminal sanction ability only on a couple of occasions and has not imposed significant civil penalties in any way. These investigations are really designed to bring some sort of formal resolution.

There is another side to enforcement and this side may be where there are more "teeth" to the Privacy Rule than what may occur through a federal office for civil rights. Beyond formal or informal approaches to addressing violations pursuant to the Privacy Rule are: Judicial uses of the Privacy Rule as a *per se* standard for what is expected for protecting health information privacy has been very interesting because there are state claims that can be brought for privacy breeches. If those privacy breeches can be framed as violations of the national standard for protecting privacy set forth in the Privacy Rule, there is more impetus for success on such a complaint. It is a way in which the Privacy Rule is converted to a national standard that can allow for certain types of sanctions. There are contractual obligations as well to adhere to the Privacy Rule. For example, business associates and limited data sets do convey various contractual obligations. If such a contract is breeched, a lawsuit can prevail. Institutional, corporate, and organizational policies that are highly consistent with the Privacy rule require adherence as well. Again, if there are breeches, people may lose their jobs, be sanctioned, et cetera. This is not to say that the Privacy Rule has no real "teeth" to it, but it to say that it is not through the federal government through which those teeth are really implemented.

With regard to the impact of the Privacy Rule on public health, consideration must be given externally to how the Rule impacts the flow of identifiable health data into or out of public

health agencies. Internally, consideration must be given to the ways the Rule affects the practice of public health or public health research conducted by public health agencies or its partners. The external issues are probably the most profound for public health because the types and places that CDC or state partners may want to go to obtain these data for a public health surveillance system are very likely going to be covered entities. Hence, consideration also must be given to what the covered entities' ability to deny data or restrict data flow.

While there are many exceptions to the Privacy Rule, it does contain what is known as the "Public Health" Exception. The "public health" exception to the anti-disclosure rule states that a covered entity may disclose PHI without specific, individual authorization to a "*public health authority* that is authorized by law to collect and receive such information for the purpose of preventing and controlling disease, injury, or disability, including . . . reporting of disease . . . and the conduct of public health surveillance . . . " Basically this clause says, "Covered entities are not in their right mind to deny access to these data for public health surveillance purposes to public health authorities. They have a legitimate right to these data. It is part of the balance of what we are attempting to do with the Privacy Rule. Give it to them if they ask for it and they have some claim to it pursuant to some authorization of law that does not have to be specific to the actually type of surveillance. It is just a generalized claim that is intended to do exactly that."

Beyond this general authorization, additional, specific public health-based exceptions include:

- ❑ Disclosures to maintain the quality, safety, or effectiveness of FDA products
- ❑ Disclosures to notify persons exposed to communicable diseases
- ❑ Disclosures concerning work-related injuries
- ❑ Disclosures about victims of abuse, neglect, or domestic violence
- ❑ Disclosures for health oversight activities
- ❑ Disclosures to prevent serious threats to persons or the public

A "public health authority" is defined as an "agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency . . . that is responsible for public health matters as part of its official mandate." Public health authorities under this type of rule include: CDC, FDA, NIH, State or Tribal Health Departments, Local Health Departments, Contractors / Others acting under authority of these agencies. A private sector entity collecting data under a granted authority from any level of governmental public health agency is viewed as a public health authority under this act. Professor Hodge highlighted this component, given that it is not well understood.

In terms of state public health reporting laws, the Privacy Rule does not pre-empt (or override) state law that "provides for the reporting of disease or injury . . . or for the conduct of public health surveillance [or] investigation . . . ." The Privacy Rule has nothing to say about state public health reporting laws because it is a privacy act. It does not restrict, allow

for, or require different data disclosures. It simply regulates the privacy between exchanges. Existing state reporting laws are, therefore, still full and effective.

Regarding the impact of the Privacy Rule on public health internally, an essential message that is beneficial to know is that, to the extent that public health authorities use or disclose identifiable health data for public health purposes, they are not "covered entities," and are thus not required to adhere to the provisions of the Privacy Rule. Simply stated, public health authorities doing public health things are not covered by the Rule. The Rule has nothing to say about what public health entities do with data internally until those public health authorities start to act like, look like, or do things that approximate what a health provider or health insurance plan might do. That is, a profound area of potential impact concerns the activities of public health authorities that resemble the provision of health care (e.g., direct delivery of health services to disadvantaged individuals) or administration of health plans (e.g., state "well person" programs). Public health authorities performing health care activities or acting as a health plan are engaged in "covered functions," and accordingly must adhere to the Privacy Rule.

Most public health authorities at the state and local levels declare themselves as hybrid entities (or multi-functional organizations with covered entity components) pursuant to the Rule. Johns Hopkins, for example, has elected hybrid status. This allows their hospital to be viewed as a covered entity, but does not require the School of Engineering to be viewed as such. Absent the election of hybrid status, an entire enterprise is viewed as covered by the privacy rule. For state health departments that have only a component of what they do considered to be a health provider type function, electing hybrid status would make only that part of the entity be required to adhere to the Rule. Simply stated, the practical effect of hybrid status is that the public health agency designates those components of its practices that are covered, and adheres to the Rule concerning those components. Others within the agency may not have to adhere to the same requirements concerning their duties, although the agency is responsible for their compliance with covered applications.

In terms of distinguishing public health practice versus research, the HIPAA Privacy Rule provides different standards for disclosing PHI without authorization for public health versus research purposes. Professor Hodge stressed that he is working with federal, state, and local officials and others to help simplify the distinctions. As well, the Office for Human Research Protections (OHRP) will soon release new guidance that may also help draw distinctions between public health practice and research.

Part of the impetus for clear distinctions relates to the fact that the HIPAA Privacy Rule standards for providing data without authorization for public health purposes are much broader than those concerning disclosures for research purposes. Disclosures for research purposes are more restrictive. Absent some narrow exceptions, research disclosures require IRB or Privacy Board agreement that the use or disclosure of PHI involves no more than a minimal risk to individual privacy based on an adequate plan to protect the identifiers from improper use and disclosure; an adequate plan to destroy identifiers as soon as possible; and adequate written assurances that PHI will not be reused or disclosed to anyone else except as required by law. There are other provisions as well. Some access to

data may be allowed without written authorization for preparation to research, for research on decedents, and for limited data sets (e.g., basically stripped down of all of the 18 HIPAA identifiers—virtually useless to many public health authorities).

The key issue is that neither the HIPAA Privacy Rule nor the federal Common Rule (regulating the performance or funding of human subjects research by most federal agencies) clearly distinguishes public health practice activities from research activities. Multiple dilemmas arise as a result: Public health practice activities that assimilate research activities, such as some types of surveillance, may be seriously misconstrued; Covered entities may deny access to PHI to public health authorities on the grounds that the requested basis for the data is research, and not practice. Public health practice activities may ultimately be submitted for IRB approval as if they are research. Public health practitioners do not have the money or the time to be seeking IRB approval for routine, public health activities.

Professor Hodge briefly walked participants through the publication titled, "A Report for Public Health Practitioners Including Case Studies and Guidance for Making Distinctions." This guidance was sponsored by the Council for State and Territorial Epidemiologists (CSTE) and is available in full on the CSTE website. The principle objectives of the guidance are to: assess legal and ethical environments underlying public health practice and human subject research; clarify existing definitions of public health practice and research; provide meaningful cases on practice and research; and make distinctions between public health practice and research through foundational and enhanced guidance. Professor Hodge stressed that this is of great importance to ALS / MS surveillance systems because of what they may be doing with the data. If the next step to acquiring the data is to engage in systematic research using the data, this could have implications with respect to the various entities being willing to provide the data.

The guidance provides functional definitions where there are none. "Public health practice" is defined as the collection and analysis of identifiable health data by a public health authority for the purpose of protecting the health of a particular community, where the benefits and risks are primarily designed to accrue to the participating community. This definition relate to the context of public health authorities attempting to acquire large amounts of identifiable health data through covered entities. It is the collection and analyses of those data by public health authorities for the purpose of protecting the health of a particular community, where the benefits or risks are primarily designed to accrue to that participating community. In contrast, "public health research" is defined as the systematic collection and analysis of identifiable health data by a public health authority for the purpose of generating knowledge that will primarily benefit those beyond the participating community who bear the risks of participation.

This publication includes a checklist that offers a way to make simple and then more difficult distinctions between practice versus research in an effort to bring some consistency to the approach. This checklist was built by noting that there are some core essential features of foundations of practice versus research that are very different. If these are assessed through the checklist, one can quickly distinguish many cases. For the more difficult cases,

the ones that look a lot more like research and it is very hard to determine what public health authorities are actually doing with the data, there are enhanced guidelines to provide some clarity.

Foundations of public health practice drive public health authorities to do what they do in the collection of identifiable data, and this often: 1) Involves specific legal authorization at the federal, state, or local levels (for example, a state legislature commands public health authorities to collect certain data); 2) Includes a corresponding governmental duty to perform the activity to protect the public's health; 3) Involves direct performance or oversight by a governmental public health authority (or its authorized partner) and accountability to the public for its performance; 4) May legitimately involve persons who did not specifically volunteer to participate (i.e., they did not provide informed consent); and 5) Is supported by principles of public health ethics that focus on populations while respecting individual rights.

In contrast, the foundations of human subjects research: 1) Involves living individuals or identifiable information about them; 2) Involves identifiable data that are not publicly available or for which the individual has not already consented to their use for research purposes; 3) Involves research subjects who voluntarily participate (or participate with the consent of their guardian), absent a waiver; and 4) Is supported by principles of bioethics that focus on individual interests while balancing the communal value of research.

Professor Hodge stressed that of the cases analyzed, these foundational principles were very clear in distinguishing practice versus research activities. Nevertheless, because of the multifarious approaches used at all levels (e.g., universities, public health sectors, IRBs, et cetera) very broad mistakes are being made nationally. Hence, these foundations do not resolve all issues. While there are numerous existing principles currently used (e.g., intent to publish, urgency, et cetera), these were found to be non-helpful in distinguishing practice from research. In order to deal with the difficult cases that cannot be resolved simply, enhanced guidelines are included in the CSTE publication to help further distinguish practice from research:

- General Legal Authority: Is there some general legal authority for the performance of the activity?
- Relationships / Accountability: What is the proposed relationship of the actors to those participating in the activity? Who is accountable for the health and safety of participants?
- Specific Intent: What is the specific intent of the actors performing the study? This is what presently drives some of what CDC uses to make determinations between practice and research.

Unfortunately, it has been found consistently that specific intent can be greatly manipulated. Intent can become whatever someone wants it to be depending upon what they feel they have to do. A research activity can be framed as a public health practice intent, which is what is occurring nationally and at the state level. Intent is a valuable element in distinguishing practice from research, so there must be specification of the types of intent. The criteria in the CTSE guide are as follows: 1) The intent of research is *to test a*

hypothesis and seek to generalize the findings or acquired knowledge beyond the activity's participants; and *2)* The intent of public health practice is *to assure the conditions in which people can be healthy through public health efforts that are primarily aimed at preventing known or suspected injuries, diseases, or other conditions, or promoting the health of a particular community* [language from the Institute of Medicine (IOM)]. If a project can be framed with one of these intents versus the other, this offers the ability to make a stronger claim about what type data is being required for what purpose. Beyond that, some additional criteria included in the guide which may be beneficial are:

- What are the participant benefits? Is the activity designed to produce some benefit to the participants or their population?
- What are the interventions involved? Is the activity designed to introduce some non-standard or experimental methods or analyses to participants or their identifiable data? If so, it is by definition, research.
- What about subject selection? How are the participants selected? Is it through a random selection so that the results of the activity can be generalized to a larger population?

This approach is built into the following checklist, which is designed in a two-page format to help a public health authority walk through these criteria, and which should provide additional ways to make better, consistent, uniform distinctions between practice and research:

- Step 1 - Check Key Assumptions
- Step 2 - Assess the Foundations of Public Health Practice
- Step 3 - Assess the Foundations of Human Subject Research
- Step 4 - Consider Enhanced Guidance
- Step 5 - Conclusions

Hanging in the balance is access to the data. If data are being sought for research, more privacy laws designed to protect people in human subjects research will be in effect, as contrasted with showing that data are required for public health practice activities.

That being said, Professor Hodge reported that a key update for considerations is that presently, the Office for Human Research Protections (OHRP) is working internally with federal agencies to review the bases for distinguishing research and non-research activities significantly, including public health practice activities. OHRP is expected to release new guidance on these issues for public review and comment later this year. This will be published in the Federal Register, with public review and comment available. This will be momentous for attempting to get a better sense of how to make these decisions.

In conclusion, Professor Hodge reiterated that the HIPAA Privacy Rule presents national health information privacy standards and creates a floor, not a ceiling, for privacy protections. Existing legal protections at the federal or state level may remain effective provided they do not conflict with the Privacy Rule. The Rule impacts public health in practice, research, and health care / plan capacities in multiple ways. Though not entirely clear, distinguishing public health practice and research is essential to the application of the Rule. For more information, Professor Hodge invited those present to contact him at jhodge@jhsph.edu.

Discussion Points:

- Dr. Williamson complimented Professor Hodge on a marvelous job of delivering this information in such a palatable manner, particularly given that it is typically considered to be such a dry topic. He inquired as to whether the OHRP planned to collect input from public health agencies in order to better understand how to facilitate agencies in conducting their work in a more flexible fashion.

- Professor Hodge responded that OHRP is currently engaged in a process to solicit review and comments from all HHS entities. They have met with CDC officials in Washington several times to gain their feedback and to assess what the proper approaches would be. Unfortunately, they have not extended that to anyone outside the federal government. For example, CSTE and other private entities do not have access to this process. When it is published in the Federal Register, by law they have to open it up for public comment and review, which is when those across all public health sectors will have an opportunity to review and comment upon what is published. He worked closely with OHRP on the CSTE project and found their focus and perspective to be very different in that they are required at the federal level to enforce the Common Rule. To the extent to which OHRP has to enforce the Common Rule in a heavy-handed way, they will do so. Hence, if OHRP believes that a certain type of activity could be viewed, even in a small way, as research—it is research and the Common Rule applies. OHRP is working in a way to try to explicate that, which could be helpful. Though convinced that OHRP would receive excellent advice from various public health agencies, it was not clear to Professor Hodge that OHRP would craft a method for distinction that would allow public health practitioners to do what they traditionally do with these data without some type of IRB oversight. His prediction was that OHRP would take a broader approach to the definition of what constitutes “research.” They have already shown some unfortunate misunderstandings about what public health surveillance is as contrasted with research; however, he stressed that until the criteria are actually

published, he could not comment fully. It is not that they do not "get it." They do, but their job is to enforce the Common Rule and they will do that to the highest level they can to ensure that human subjects are not involved in certain activities in which they could be harmed.

- Dr. LaRocca requested that Professor Hodge expand on the concept of "community." It could be defined geographically as well as in other ways, and it seemed as though the distinction between research and practice hinged partially on the benefits to a community versus acquisition of knowledge in general. Professor Hodge replied that there may be various justifications for surveillance practices, for example, because of the potential national impact of these data. Someone may be, through a single surveillance practice, acquiring some data even in a limited geographical area which has direct benefits to persons with similar conditions in the rest of the nation or even internationally. In his view, this would constitute a legitimate public health practice under this standard and from his perspective, the community was not defined in a geographically limited way. It is defined in a way that the purpose or what drives the underlying activity is to provide direct benefits to the community about which these data are being acquired. That could be a subset of a community or the entire community.

- Dr. Pentz inquired as to how to target a community that does not have increased risk but the information gained would benefit the larger public health effort because the regulations seem to imply that one can only survey "at risk communities that have the potential to benefit form the surveillance".

- Using HIV / AIDS as an example, Professor Hodge responded that part of the reason they acquire these data is to prevent transmission to persons who may potentially be at risk. This is done by acquiring data and learning more about index cases so that a better assessment can be made about how HIV / AIDS is transmitted in various cases and how public health authorities can intervene before it happens again. Community is much broader than the persons about which information is in the systems themselves.

- Dr. Kasarskis said it sounded as if they were making all of these distinctions and asking public health activities essentially to "stick their head in the sand." With that in mind, he wondered how they could analyze community data for anything without generating a hypothesis. It seemed to some degree that they were being asked to collect data that would be beneficial in a practical way to a specific community, however that is defined, and not asking anybody to come up with a new idea of what relationships might be from that. In order to engage in a good public health, responsible, ethical function, one would have to think about the data, see relationships, and consider how generalizable that might be.

- Professor Hodge stressed that he did not intend to give the sense that this approach was restricting the ways the data could be used for surveillance purposes. In fact, the approach is about attempting to find a way to distinguish practice from research at the point of data collection so that there are not covered entities within the HIPAA saying, "We used to see this type of data that you are asking for as a public health thing, but we see it more now as research. As a result we're going to demand that you obtain some sort of IRB approval." That is not a legitimate conclusion of the Privacy Rule. They are not in charge of making that distinction. If a public health authority says something is a public health practice activity, they can acquire the data for that purpose. It is about providing a legitimate justification, based on thinking through the activity and making a determination based on the criteria, that it is a public health practice activity. The Privacy Rule does not cover public health authorities doing non-covered things. Once the public health authority gains access to the data, the CE is out of the equation as long as they handed it over to a legitimate public health authority for a legitimate public health purpose. What the public health authority goes on to use those data for is regulated under various standards, not the Privacy Rule. Research interests may come into play later for which the authority may have to seek IRB approval, but it does not stop the CE from giving those data merely because this may occur down the road for a research purpose.

- Referring to the definition of "public health research," Dr. Schmidt asked for some examples as she was unclear of "benefits beyond that community."

- Professor Hodge replied that in addition to what he would give, there are many examples within the report itself. HIV / AIDS is one example. If HIV / AIDS data are collected legitimately for surveillance, but it is discovered that there is a strong link with the spread of another sexually transmitted disease (STD), to the extent to which some comparative analyses need to be done, HIV / AIDS data bases can be compared with syphilis or tuberculosis data bases, for example. Assuming that there is nothing wrong about how the data were acquired, the potential to use those data within the public health entity to provide certain analyses to generate knowledge that will benefit persons who are not within the HIV / AIDS data base, but could be implicated within the tuberculosis setting, is where they are starting to explore how public health entities use those data to benefit persons outside the individuals within that context. Without taking on a very specific data use proposal, Professor Hodge pointed out that it would be difficult to go beyond a very general answer. Although public health authorities should not be bootstrapped to use an HIV / AIDS data base solely to benefit persons with HIV / AIDS, sometimes when those data are coupled with other data or are used to extrapolate certain analyses or hypotheses, at some point that can shift from practice to research. OHRP is really concerned with the shift from practice to research. All that means is determining at what point IRB approval must be sought for the type of data use. It is not about saying that if practice does shift to research, the data cannot be acquired at all.

- Dr. Sorenson pointed out that under the existing Privacy Rule, if a public health agency establishes a registry or a data base, they can disclose that unidentifiable data to a researcher as long as they have approval and oversight by an IRB. Most universities have federal wide assurances, although not all freestanding IRBs do. The oversight that those provide as quality of the protection can be very different. He wondered if that made a difference at all in terms of the HIPAA guidelines in terms of who they can disclose information if the degree or level of oversight of protection is provided at the other end. Professor Hodge responded that it could make a difference, not so much pursuant to the HIPAA Privacy Rule, but rather to the Federal Common Rule.

Overview of Human Subjects Protections — February 7, 2007

Anne Sowell, PhD
Chairperson, IRB A
Associate Director for Science, Division of Health Studies
Agency for Toxic Substances and Disease Registry

Dr. Sowell indicated that basically, three questions must be answered to determine whether IRB approval is required: 1) Is the use of the data research?; 2) Does the use of the data involve human subjects?; and 3) Is the use of the data exempt human subjects research?

With respect to whether a proposed activity is research, the federal definition of *research* is "a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. Activities which meet this definition constitute research for purposes of this policy, whether or not they are conducted or supported under a program which is considered research for other purposes" [45 CFR 46.102(d)]. If activities are supported by federal funds, OHRP definitely has a say in it.

The purpose of the ALS / MS activity is to answer the question "Which of the national datasets are useful in identifying cases of ALS or MS?" ATSDR / CDC has determined that the initial activity is not research because it is asking one specific question and it is not generalizable. However, individual institutions may disagree because the activity may involve research from their perspective. OHRP does allow for disagreement between IRBs. Each institution has the right to make their own decisions about whether an activity is research or non-research. One exception is if ATSDR / CDC funds an activity and declares it to be research, then the grantee is obligated to treat it as a research activity. If the data to be used were collected as part of a research study with IRB oversight, then the use of the data may require approval by the IRB even if the activity is considered not research. The reason for this is because identifiable data collected under IRB oversight can only be used for the purposes specified in the protocol and consent documents unless the IRB gives approval. Data collected under IRB oversight remains under IRB oversight until the IRB gives up oversight of that data, which may occur if data becomes anonymous. Dr. Sowell acknowledged that because most of those present are engaged in activities that do not allow the data to be anonymous, this is not really relevant.

Pertaining to whether a proposed activity involves human subjects, the federal definition of *human subjects* is "a living individual about whom an investigator (whether professional or student) conducting research obtains: 1) Data through intervention or interaction with the individual; or 2) Identifiable private information" [(45 CFR 46.102(f)]. The ALS / MS pilot activity does not involve identifiable data. ATSDR is not using identifiable data and the grantees will not be providing identifiable data in this situation. Therefore, it is not a human subjects activity. The pilot projects are using identifiable data at their local sites because the only way to link the data sets is to use identifiable data.

An activity could be considered exempt if the data being used is anonymous. Exempt research is defined as research involving the collection or study of existing data, documents, records, pathological specimens, or diagnostic specimens, if these sources are publicly available or if the information is recorded by the investigator in such a manner that subjects cannot be identified, directly or through identifiers linked to the subjects [(45 CFR 46.101(b)(4))]. It is unlikely that the ALS / MS activity meets the criteria for exemption since datasets must be linked by patient name.

What this means is that if a site has determined that the project is research, IRB approval will be needed. If a site has determined that the project is not research, but the data being used were collected under IRB oversight, IRB approval may be needed. If a site has determined that the project is not research and data being used are not from IRB approved studies, IRB approval is not needed. If the activity needs IRB approval and the entity is HIPAA covered, a waiver of HIPAA authorization must be requested. If the activity does not need IRB approval, an institution may still require a HIPAA waiver to be obtained. However, this is not an overwhelming burden. At least for the ALS projects, most of the sites' IRBs have determined that this is human subjects research. If it is considered research and IRB approval is required, then HIPAA approval will also be required because the local site is a covered entity. Some institutions have gone overboard with the HIPAA determination and required HIPAA waivers for any use of data for anything that they could vaguely construe as research.

A request may be made for an IRB to grant a waiver of consent for an activity if:
1) The activity represents minimal risk to the people whose data will be used; 2) The use of this data will not adversely affect the rights and welfare of those people; 3) The activity could not be conducted if each person had to provide consent; and 4) If relevant data is generated from this project it will be disseminated through publications and presentations. The only time a waiver of consent cannot be requested is if there will be an ongoing relationship with participants temporally associated with the activity.

Certainly, IRBs vary in how well they protect human subjects; however, OHRP considers all IRBs to be equal. Therefore, everyone must work within the constraints of their own IRBs. The IRBs for the pilot studies have all determined that this is research. The overall project is the surveillance activity. ATSDR / CDC considers surveillance to be non-research; however, if registries contain enough data to be useful for research activities, they prefer these to be considered as research registries. Dr. Sowell pointed out that while she had not

seen what final elements would be included in the registry, if it is broad enough that it could be useful for research, the registry will have to be considered as a research registry. Her understanding from Dr. Kaye is that there will be very few elements actually collected from each participant in the registry. This is a characteristic of surveillance. Surveillance generally collects minimal amounts of data to provide information about prevalence, incidence, basic demographics, et cetera. At CDC, whether an activity is considered research or surveillance is defined by the amount of data being collected.

Discussion Points:

- Dr. Kasarskis said it seemed if this was operationized in actual practice, functionally most people are interested in the research questions. That is what patients are asking, "Is there something in the environment?" "Is there something that I've done that has brought this disease on?" This is a theme running through the public's mind. Presumably that is where activities like this should go. Therefore, the default of labeling this up front as a research activity satisfies many of these issues. One thing he did not hear in this presentation was anything about the default clause pertaining to a participant withdrawing consent. This is difficult to operationalize because once the "toothpaste is out of the tube," it is gone. He wondered how that played into this, how withdrawn consent would be handled, and if it was a "smoke and mirrors" clause or if it could actually be done.

- Dr. Sowell replied that to some extent it is a "smoke and mirrors" clause unfortunately. Once the data is in a registry, once data has been analyzed, the "genie cannot be put back in the bottle." If information is being collected to determine the number of cases in a given year, somebody cannot say their name was submitted and they do not want to be included. While the name itself can be deleted, the information about the case will not be deleted. Dr. Williamson added that for future analyses, that name and number can be deleted. Dr. Sowell agreed, but stressed that there would always be a trace of that information in the dataset even if there was no further follow-up on that case. HIPAA indicates that data may be removed for future analyses, but existing data may not be removed.

- Professor Hodge stressed that this was an important point from a public health standpoint. From a public health perspective, what they do not want to have to do is go back to seek individual authorization. No one has the time or money in public health to do that for several research applications in which they want to engage. The reality is that there are ways to continue to use public health data for research purposes without written authorization provided and IRB will agree to these various minimal impacts on privacy and adequate plans being set up. That is the way in which they should attempt to accomplish this, given that the risk of having people opt out of further study could be so damaging, expensive, and deleterious to the overall effects. While there is a compelling reason to do this, some IRBs may not agree to it.

- Dr. Sowell has found that if completely honest with people about why the activity is being conducted, the average person cares a lot less about protecting their privacy and their

rights than the IRB or HIPAA boards do. Most people are a lot more willing to offer more data than realistically should be asked, especially because people in communities affected by illness want a reason they are ill and they want a cure to be found. However, it takes only one person having their data misused to have an entire community turn against you. Therefore, if they are honest and they let people know that the data are being given to ATSDR when that is relevant and practical, there should not be repercussions and people are not likely to withdraw from registries.

- In the context of the ultimate goal of developing a surveillance system for chronic neurological disorders, Dr. LaRocca wondered what the downside would be to considering this to be research other than that it would have to be regulated by IRBs.

- Dr. Sowell responded that the greater downside is HIPAA. IRBs will approve data use for a variety of things, especially if lack of adverse impact on the subjects can be demonstrated. It becomes harder to populate a dataset if they have to tell entities that they are collecting the information for research purposes. HIPAA kicks in and a lot of the healthcare institutions are still very protective of their data when this occurs. Research authorizations are permitted only with a HIPAA waiver, which is the greatest barrier to having this considered to be a research dataset. Currently, the IRB issue is in limbo given the activities of OHRP. It is not clear which way they are going to swing on public health research versus public health practice. In OHRP's first draft of the Rule, they were very restrictive on what would be considered research. Unfortunately, many of CDC's activities for which the agency has fought long and hard to have considered as practice fell into the research category, which is disturbing.

- Dr. Kasarskis pointed out that with ALS, they are dealing with a condition that will be fatal on the average in four years; that is, 50% of their patients will have died by that time. Reflecting on the distinction about the decedents' data that may have been gathered when these persons were alive, Dr. Sowell requested additional information on the boundaries following the subject's death. With respect to genetic issues and the importance of the data to a deceased subject's family potentially for their future insurability, he thought he understood that those data would pass more easily into a research realm than if gathered on a live subject.

- Professor Hodge replied that there are different, more permissive ways, to gather data about persons who have passed away for research purposes because the privacy expectation is diminished. It is not gone, however, because the family still has some expectations. There are ways to obtain more access to those decedents' data than would be true for living individuals. Under the Privacy Rule this is definitely the case, and under the Common Rule these people are not covered. It is not research at this juncture. With respect to passing more easily into a research realm and Dr. Kasarskis's point about genetics, Professor Hodge stressed that there is one caveat in that states have very extensive and often very restrictive genetics laws that are must stronger than what is set forth in the Privacy Rule. Therefore, states may very well clamp down on any type of genetic data being circulated pursuant to a descendent or otherwise. Dr. Sowell added that some IRBs are looking at family members as secondary participants with respect to genetic studies.

- Dr. Sorenson pointed out that if investigators obtained consent, some of these issues should not pose problems. Dr. Sowell replied that the easiest way is to obtain consent from people. For those who have large datasets, especially if people are deceased or are no longer patients, it is not practical to go to each of them to request permission to use data for another project, so waivers will be needed. When there is an ongoing relationship with a potential participant, consent or signed HIPAA authorizations are required.

IRB and HIPAA Issues from a University Perspective — February 7, 2007

Rebecca D. Pentz, PhD
Professor of Research Ethics
Winship Cancer Institute, Emory University

Dr. Pentz stressed that the reason there is so much regulation in this country is because we earned it due to a great deal of previous research abuse. She reported that IRBs were instituted in the 1960s after repeated research abuses were discovered, for example: San Antonio Contraceptive Study; Willowbrook Hepatitis Experiments; and Henry K. Beecher's expose "Ethics and Clinical Research" *NEJM* June, 1966 (Lists 22 unethical published studies).

The premise of the Health Insurance Portability and Accountability Act of 1996 is good (e.g., patients' private health information should be protected). To illustrate that HIPAA had really been around for a very long time, Dr. Pentz quoted an "oldie but goodie" from the Hippocratic Oath, 5th Century BC, "Whatsoever I shall see or hear in the course of my profession, as well as outside my profession, it is be what should not be published abroad, I will never divulge, holding such things to be HOLY SECRETS." She said that "Holy Secrets" was really the old way of saying "PHI." Thus, HIPAA is well-founded philosophically.

Dr. Pentz pointed out that academic medicine differs from other settings in various ways. Part of this has to do with scale. CDC has seven IRBs, while Emory University has five. True about all IRBs is that they all have their own characteristics depending upon the membership, which causes numerous issues. Emory's IRBs function as HIPAA authorization boards; that is, if someone wants a HIPAA waiver, they would seek that from the IRB. Emory also has the resources to formalize most requirements. Each of the following links leads to a form that an investigator can fill out, so no investigator can make any excuses for not knowing how to complete the forms if they can figure out which forms they need:

HIPAA Forms

HIPAA Assurance Regarding Disclosure of a Decedent's PHI for Research Purposes
HIPAA Authorization Form for Use and Disclosure of Protected Health Information for Research Purposes\
HIPAA Authorization for Use/Disclosure of Protected Health Information by Emory University to a Third Party
HIPAA Authorization for Use/Disclosure of Protected Health Information From a Third Party to Emory University
HIPAA Authorization for Use/Disclosure of Psychotherapy Notes by Emory University to a Third Party
HIPAA Business Associate Agreement
HIPAA Business Associate Confidentiality Agreement
HIPAA Business Associate Security Agreement
HIPAA Consent and Authorization for Protected Health Information to be Included in a Research Database
HIPAA Data Use Agreement
HIPAA Illustrations of Situations Requiring/Not Requiring Authorization
HIPAA Listing of Typical Business Associates
HIPAA Log to Track Disclosures of PHI
HIPAA Patient Authorization for Use and Disclosure of Protected Health Information
HIPAA Patient Complaint Form
HIPAA Patient Consent for Use and Disclosure of Protected Health Information for Treatment, Payment and Health Care Operations Purposes
HIPAA Patient Consent to Means of Communication
HIPAA Patient Denial Letter
HIPAA Privacy Policy Training Checklist
HIPAA Privacy Representative's Incident Event Log
HIPAA Receipt of Notice of Privacy Practices Written Acknowledgement Form
HIPAA Request for an Accounting of Certain Disclosures of Protected Health Information for Non-TPO Purposes
HIPAA Request for Correction/Amendment of Protected Health Information
HIPAA Request for Limitations and Restrictions of Protected Health Information
HIPAA Request to Inspect and Copy Protected Health Information
HIPAA Workforce Confidentiality Agreement

IRB HIPAA Forms

IRB: Combined Informed Consent/HIPAA Authorization
IRB: HIPAA Authorization Revocation Letter
IRB: HIPAA Stand-Alone Authorization Template
IRB: HIPAA Worksheet/Application for Waiver of Authorization

Emory is considered to have "deep pockets," so they do get sued. In one of the latest cases they have had, Emory employees were privately subcontracting with a public health agency to conduct research. They were using a reportable disease database, which is where they obtained their information. They were doing cold calling using an Emory phone bank, so when people received the call it said "Emory University" on their caller identification. One person saw "Emory University" on their phone who did not have the disease the investigators were calling about, had no idea why they were in the database, and subsequently sued Emory. Hence, the Emory lawyers are reasonable, but they are cautious.

HIPAA was expensive for Emory. Start-up included $463,000 for outside counsel for HIPAA analysis, 75% of an in-house counsel's time for a year, and it continues to cost major dollars for the work that they are doing. Other on-going costs include continuous risk analysis, updating of all electronic software, and monitoring against confidentiality threats.

There are confidentiality threats. A laptop with Emory patient PHI was stolen from a private contractor. Emory sent out a letter to all patients explaining how to find out whether there has been any breech in their confidentiality. In a similar situation with the University of Pennsylvania, the university paid for all credit checking. However, Emory did not do this. In another incident, a subcontractor lost a USB pin with Emory patient information.

Another major difference between an academic medical center and other settings, particularly public health, is that the focus of the academic center and of the IRBs (even though they have an excellent school of public health and they live right down the road from CDC) at Emory is on the individual patient. It is very difficult for them to see public health kinds of issues. Personal autonomy is the bedrock principle, even to the extent that it gets in the way of a lot of other issues. Medicine is based on the physician-patient dyad. The core ethical principle is respect for individual autonomy. That is, public health ethics is not the coin of the realm in academic medicine. Even with all of the public health that surrounds them, this is why Emory's IRBs and researchers will be focused on individual patients.

Also different in an academic versus other settings is that the culture of academic medicine is hierarchical with tenured professors at the top. There is no doubt that the hierarchical, tenured system is a medieval caste system. Caps and gowns became the official academic dress proclaimed in 1321 AD, and this has not changed at all. What that means practically is that in hierarchical systems, it is easier to get a project approved by working laterally (e.g., professor to professor, physician to physician, PhD to PhD, epidemiologist to epidemiologist).

Academics can be arcane and they consider themselves experts—sometimes a panel of experts is not needed, yet IRBs are full of panels of experts. For example, a sociologist criticizes an oncology protocol as too invasive when it actually is just beyond the standard of care. Or an oncologist criticizes a social science questionnaire as too sensitive. Sometimes, even though they are experts in their field, they have no clue about what the standard of practice is in other fields. Nevertheless, the times are changing. Academic institutions are becoming more entrepreneurial. It is amazing how much money one can make in academic medicine currently. Tenure is not as important anymore as fame and fortune. For example, Dr. Pentz just reviewed a case of an assistant professor who has never written a successful NIH grant, but who runs a small biotech company where he is making multi-millions and has eight employees.

Emory has a full-time HIPAA expert who makes all of the decisions. Dr. Pentz visited with her to explain the discussions in the March ALS / MS workshop. The Emory HIPAA expert declared it to be research and said that it has to follow the rules as they stand. Therefore, what is needed to use Emory patient information in a database for a retrospective study is that data must be de-identified or include a limited data set (dates, city, state, zip). For a prospective study, they must have consent and HIPAA authorization. Either must have IRB approval. That said, because they are academic, if a cogent, well-argued analytical case, Dr. Pentz's experience is that the IRB and their HIPAA authority will respond to it because they are moved by concepts. One of her jobs at Emory is when a person has an excellent idea, but which is a little "squiggly" on the regulations, she puts together the case to show that it should move forward as a public health activity. They often "win the day." Therefore, it is not impossible to move this registry forward, but they may have to make a compelling argument that it is not research.

Discussion Points:

- Dr. Kasarskis thought this got down to a point of law because it sounded as though, if Congress decided legally that ALS and MS are public health problems which need to be solved with a public health approach, the proposed system presumably would be removed from some of these considerations.

- Using cancer as a model, Dr. Kaye pointed out that when Congress decided there should be a war on cancer, one way to do this was through a cancer registry. Congress awarded funding to CDC to start a cancer registry, and there was a requirement that to obtain funding, each state had to make cancer a reportable disease. Many of the state laws do include fines and penalties for people who do not report and some have exercised that authority on occasion. Although Congress might say ALS / MS are reportable and states have to do it, that delegation has historically been given to the states. With infectious diseases it has been easier to make this argument than with chronic diseases.

- Dr. Kasarskis said during the March workshop, they concluded that this may not be a viable approach, but he wanted to understand some of the principles that would underlie what would be brought out as something broader than just the patient / physician contact and exchange of information.

- Dr. Kaye replied that she helped write the applications to places like CMS to gain access to identifiable data. The fact that someone has become interested, from a public health perspective, in obtaining information on incidence and prevalence is part of the argument for why they should have access to this information. While this does not require the owners of the data to give the information, it does make them think more kindly upon the application for it.

- Professor Hodge added that Congress really cannot push states around, but they can attach it to funding. The important aspect from the HIPAA Privacy Rule perspective is that at the state level, they do not have to line item detail that they may now collect MS or ALS data via some surveillance practice. That is not required by the Privacy Rule. They simply have to show that the acquisition of these data are in the interest of protecting the public's health and that it is done by a public health agency or a contractor of a public health agency. While a statutory regulation might make it easier to obtain the data, they could launch this surveillance system at the state level now with only consensus that this is a public health objective to which many states believe it is essential to contribute.

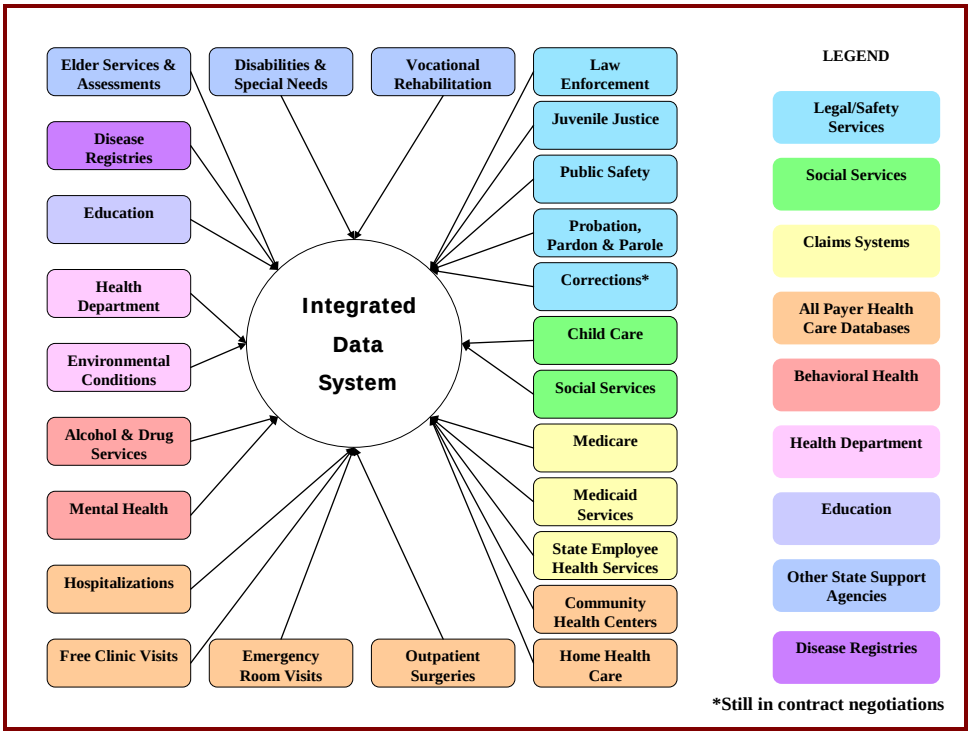
IRB and HIPAA Issues from a State Perspective — February 7, 2007

Mary Tyrell, PhD
South Carolina Budget and Control Board
Office of Research and Statistics

Dr. Tyrell stressed that her message to them was that not only are there differences with HIPAA and IRBs, but every state has different laws. When considering the conduct of a surveillance project, this means dealing with 50+ methods of data collection for a variety of diseases. Three of the most common forms of data collection include: Public Health Agencies, Other State Data Agencies, and Hospital Associations. Models for data sharing include administrative, statutory, and contractual / voluntary. She explained that her office is not a public health organization; they are strictly an office of research and statistics. They have no regulatory / statutory authority to implement, regulate, license, or in any way do anything for the systems in South Carolina. Their mission is merely to conduct data research and other functions for other state agencies, universities, and other interested parties. With respect to population-based surveillance, in a lot of the states the hospital associations collect the in-patient and emergency department (ED) data. There are other non-profit organizations collecting data as well. Complicating all of these different systems that are collecting data is that there are different models for data sharing. Some agencies,

hospitals, associations, and other entities can have the authority within their organizations to decide to share or not share data. Some of this authority is statutory, which is true in South Carolina. Dr. Tyrell must work through a legislatively mandated committee to make determinations about data sharing. If someone requesting data does not like the decision the committee makes, it can go to an administrative law judge, circuit court, and all the way up if desired. The bottom line is that no matter what type of agency or what model of data sharing is utilized, all must adhere to HIPAA and IRB as they pertain to the individual organizations.

The following illustrates the dataset to which the Office of Research and Statistics (ORS) has access:



Not only must the ORS comply with HIPAA, but also they must comply with FERPA and numerous other rules and regulations. They have the ability to link and track anyone across all of these data sets—it is extremely powerful. They have the ability to look at not only what happens when someone presents for ALS, but also if they are covered by Medicaid services, there is a record of all of the physicians' data, all the tests they have received, et cetera. That is the good news. The bad news is that there is a different method to access every single data base in this system.

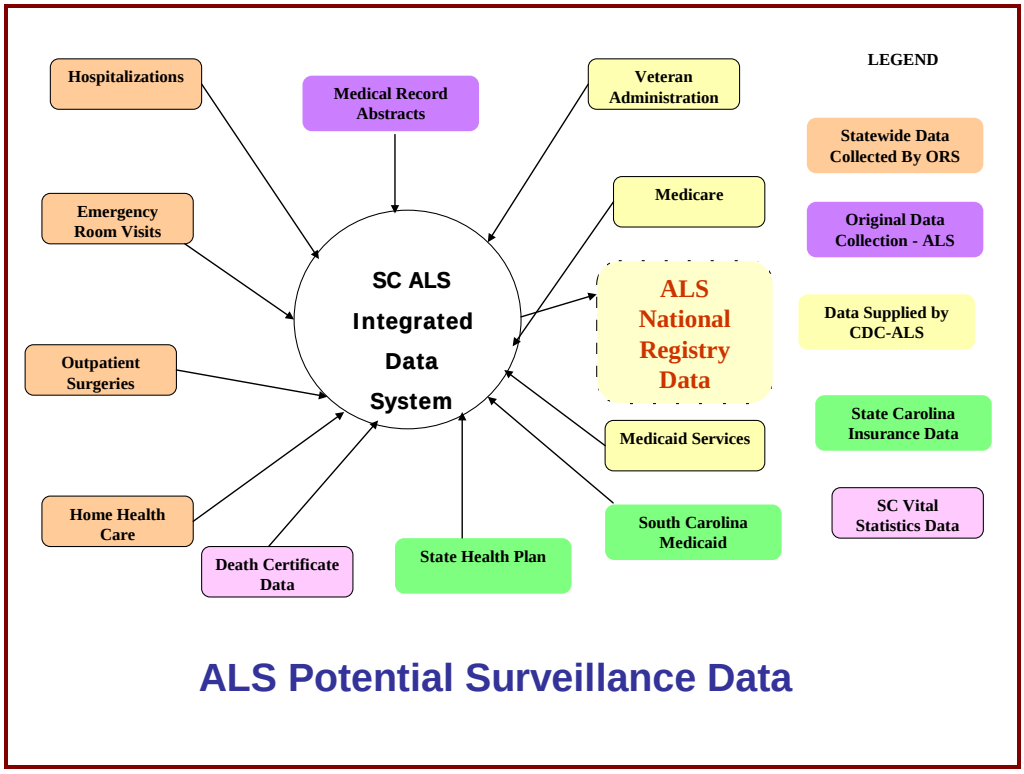
Dr. Tyrell reiterated that she cannot allow anybody to use the data without going through their formal access process. Nevertheless, South Carolina's uniqueness is that there is one entry point to multiple data sets (ORS). For a surveillance project, for example, CDC / ATSDR would contract with ORS only. The ORS staff coordinates all access to data bases. Part of the reason they choose to do that is because over the years they have developed a very good relationship with most of their data partners. Every state agency in South Carolina gives ORS virtually every data set they have, so they must be very judicious in guarding and sharing data to ensure that all of their actions are truly in the best interest of the citizens of South Carolina.

Part of what they do is administrative. South Carolina has Medicaid and a state health plan. Teachers in any school in the state, firefighters anywhere in the state, almost every county health department employee, and others are considered to be state employees. Therefore, South Carolina has more state employees than any other state, because they are covered by the state health insurance plan. Therefore, when those two data sets are linked, all healthcare encounter information is on record for 1.25 million people or a quarter of the population of South Carolina. So, the state health plan is an administrative process.

State laws guide the use of these data sets as well. This is where state laws overlay HIPAA, FERPA, et cetera for in-patient, ED, and out-patient data. There are federal programs such as Medicaid that guide that, and there are contractual limitations. With respect to medical record abstraction, because they can link and track, they can do all sorts of individual clinical data, et cetera. Researchers can provide their data and ORS can link and track it with appropriate accesses, they can de-identify it, and can give the researcher back not only their data, but also whatever other data they have requested. CDC / ATSDR receives one, unduplicated, linked dataset. There are some types of access that are really a combination of multiple levels, such as vital statistics. On occasion not only do they have to get a vital statistics approval, but also IRB and other types of approval. Therefore, it is imperative to understand that access takes time for any project.

One of the benefits of the ORS data sets is that recipients can get an unduplicated, linked data set across all of the various data sets. For example, specific to the ALS data set, Dr. Tyrell can link and unduplicate anyone who has had an ALS diagnosis or encounter anywhere in the state across five years. They can look at some who were diagnosed after the first year, pre- and post-encounters, what they came into before, what they came into after, whether they have died and if so at what point, et cetera. The beauty of all of that is ORS can combine this, de-identify it to satisfy IRBs and HIPAA, and provide it back to the person requesting it.

The following illustration depicts the South Carolina ALS project:



South Carolina will be using hospital in-patient, ED visits, out patient surgeries, and home health care. ORS has all of this information for anybody in South Carolina who was served by any South Carolina facility. They are going to add to this the death certificate, state health plan, and South Carolina Medicaid data. Although Dr. Tyrell acknowledged that Medicaid data are being obtained at the federal level, she requested the South Carolina Medicaid data because she can get access to every database that Medicaid has and all of the different types of information, including extensive eligibility information. People on Medicaid in South Carolina tend to come and go for a variety of reasons, so this helps them to look at standing: When were they eligible? One unfortunate person in their study so far has been in ORS's hospital, ED, outpatient surgery, home health care, state health plan, and Medicaid data over five years. The ability to look at this information in this manner is very powerful, especially with respect to incidence and prevalence rates, treated prevalence rates, et cetera.

South Carolina has successfully moved through all of the access issues. Their goal now is to generate the integrated database, de-identify it, and supply it back to CDC / ATSDR for this project. ORS is also adding medical records data, which means they must communicate with private providers. From the state perspective, this means that they may have to go through an IRB. ORS cannot directly collect medical records data; they must contract with the public health organization which has to collect the data, although they

cannot see the names and addresses. They have been working on a method to do this where the public health organization can see names and addresses only when the abstractor gets to the institution, physician, hospital, or wherever it is they are going to do the abstracting. Prior to that, any information must be de-identified because of some of the rules that were set up under South Carolina law, which have nothing to do with HIPAA or IRB. This adds a level of even more complexity and issues they must deal with, including additional time, which will delay the deliverables to CDC / ATSDR.

In terms of how all of this relates to computer enhancements and electronic advances that have been made, Dr. Tyrell shared several examples of what South Carolina is doing with this type of data. They have developed an electronic personal health record for all Medicaid patients in South Carolina, which is in the process of being rolled out currently to every private provider in the state. They do plan to track individual authorizations for all Medicaid patients (over 900,000 individuals), including rejections. Also, someone presenting in the ED can give authorization and the hospital can access all healthcare services they have received in any of the datasets participating in that combined collection of information.

They also have the Client Information Management System where they have linked every person receiving services in all of South Carolina's social services and state agencies. This system can be rolled out at the county level to the actual clinical or social worker, who can see every encounter that a person has had with any state agency, including the date and extensive information about what has happened to that person. This is also done by consent of the individual patient. They also have the right once they consent to retract that consent. This is all done in accordance with HIPAA security regulations. For anyone who accesses any of these entries, every key stroke is tracked and kept for six years.

With respect to what this all means, HIPAA does allow for the use of limited data sets, which is basically ORS's philosophy and is what they try to do with all of their researchers. South Carolina state law for ORS, the hospital ED data, in-patient, out-patient, et cetera pre-empts HIPAA because not only can ORS not identify a person, but also they cannot identify a physician or health care facility. While with appropriate authorization she might be able to share a hospital name with CDC, CDC cannot share it with anyone else. For patient identifiable data HIPAA requires an IRB; however, state laws have different requirements. Dr. Tyrell noted that while someone may tell her they have an IRB, she still may have to apply to seven or eight other entities requesting information. An IRB at their state level, and in other states, may make it go faster but they will still have to go through all of the access issues. She had one research project that had to go through 65 IRBs because nobody could agree. With that in mind, her message was that while they have the ability to conduct incredible research in South Carolina, all of it takes time. What used to take two to three years will now probably take four to five years simply because they must go through all of the approval processes.

Discussion Points:

- Dr. LaRocca asked what basic strategy is used by ORS to de-duplicate such a wide variety of records. Dr. Tyrell replied that they have a system called Unique ID Process, which takes multiple information from many data sets and uses them as gold standard IDs. There are other ways they can link back to eligibility files and they have them all put into a specific algorithm they use, although she said that for security and confidentiality purposes she could not disclose the details. Currently, their false positives are running about one in one million records. They have a goal to cut that at least by 10 times. They have someone working on this now and due to a couple of improvements, they believe they will be able to cut this down to about one in 10 million. They have over 100 million records in the data set, which continues to grow.

- Dr. Kasarskis inquired as to how they were able to obtain VA data. Dr. Tyrell responded that they receive Department of Defense (DoD) data who also receives data from ORS, and they receive VA data. However, the limitation is that they cannot use those data for specialized projects, for example the ALS project. This is one of the caveats on which they are working. South Carolina has extensive military and it is critical to what they do.

- Dr. Cwik acknowledged that clearly South Carolina has been very proactive on this collection of data bases, which is incredibly powerful, and she wondered how South Carolina compared to other states.

- Dr. Tyrell replied that there is no other state in the United States that can do the breadth and depth of data that South Carolina can do. There are about 44 states which collect some type of in-patient and ED data and 38 states that collect additional types of data. South Carolina's uniqueness is that they have added the social services, juvenile justice, and criminal data. She stressed that they must move beyond just health care data because so much what they do has implications in the social services, economics, and employment sectors. Dr. Kaye added that they are not aware of any other state that has a data set like South Carolina.

IRB and HIPAA Issues from a Private Registry Perspective

February 7, 2007

Barbara Teter, MPH, CHES, PhD
Director of Clinical Research and Development
New York State Multiple Sclerosis Consortium
The Jacobs Neurological Institute

Dr. Teter reported on the New York State Multiple Sclerosis Consortium (NYSMSC), which was established in 1994 to develop a durable database of demographic and clinical data to promote MS research and enhance patient care. Membership includes 17 sites in New York State, 27 investigators (MDs and PhDs), and 30 research or data coordinators (NPs, RNs, RAs, MSWs, and PhDs). The database includes 8,500 + registered MS patients and 14,000 + follow-up records. At the point of patient enrollment, it is disclosed that this information is being collected for research in compliance with IRB human subjects consent and HIPAA requirements.

The NYSMSC is governed by an Executive-Finance Committee, and data utilization is governed by a Scientific Review Committee. The NYSMSC is administered by an Executive Director, and a Director of Clinical Research and Development. Procedures and policy revisions require a membership quorum. With respect to policy, it is important to understand security and quality control. Official policies cover mandatory site activity, consortium membership requests for data forms, consortium membership submission of complete data forms, internal NYSMSC data requests, data ownership, external data requests and research collaborations, as well as a policy regarding NYSMSC revenues, and publications based on NYSMSC data. Consortium members can request their own data or data for all other sites.

In terms of data management and security, the database is physically housed at Uniform Data System for Medical Rehabilitation (UDSMR). They are a reputable location with their own privacy policies and a disaster recovery plan. UDSMR complies with all government PHI rules. Data are stored on a Microsoft SQL server.

Pertaining to data collection for the registry, the patient completes the first 24 questions (of 40 question sets) regarding demographic factors (date of birth, gender, race), reproductive factors, education, living environment, employment, family history (MS and other illnesses), and a self-assessment of function. Clinicians (MDs NPs) complete 15 question sets, which include MS symptoms (onset and current), MS types, characteristics of attacks, remissions, physiological characteristics (CSF and MRI), functional scores (characteristics), psychological characteristics, and DMT (disease modifying therapies). The NYSMSC database does include identifiers (patient initials [non-variable], date of birth, address, gender, and ethnicity). It does not include name, Social Security Number (SSN) or partial SSN. They understand that the ATSDR surveillance database is contingent on the value of pilot project and that ATSDR would be the keeper of a minimal database, including PHI.

In terms of the language on the consent form, membership sites comply with the IRBs of their individual institutions utilizing a consortium protocol. The title of the project is: The Establishment of a Patient Registry and Initiation of Related Projects of the New York State Multiple Sclerosis Consortium. An excerpt from the consent form describing the project reads as follows, "The purpose of the Consortium is to obtain a more accurate understanding of MS in New York State in terms of prevalence, demographics, functional capabilities, …. and treatment regimes, etc."

Consent includes information on site of study unique to each membership site; principal investigators' names and contact information; a statement of research; introduction and background; procedures; risks and discomforts; potential benefits; confidentiality, reimbursement, study costs, voluntary participation; alternatives to participation; new findings; authorization for use and disclosure of identifiable health information for research purposes; and patient signatures for voluntary consent to participate. Included with consent is an authorization for use and disclosure of identifiable health information for research purposes. Subjects are told the following: "Your health information may be shared with others outside the research group for purposes directly related to conduct of this research study or as required by law, including but not limited to NYSMSC investigators and designees; UDSMR; individuals responsible for general oversight and compliance activities; and government agencies with authority over the research including HHS, FDA, NIH, OHRP

The next step is expected to be participation in the national surveillance system. The NYSMSC database does not include patient names; however, unique identifiers can be linked to names and would require each consortium site to provide a name. Linking and reporting would require a waiver of consent and a waiver of authorization. For NYSMSC to report names with other identifiers to a national surveillance system, further consent would need to be obtained from each of the participants.

Discussion Points:

- Dr. Kasarskis inquired as to who pays for the NYSMSC database and how practitioners are compensated for collecting the data. Dr. Teter replied that New York State provided the funding for the initial set-up. The Consortium is receiving a small amount of funding, but is actively pursuing additional funding. Regarding practitioner compensation, they reimburse $30 per registration form and $30 for each follow-up form. The fees are the same across the state. Once they locate additional funding, they plan to increase the follow-up fee. The target for that compensation is to retain someone in a physician's office to ensure that the physician is completing the information. That person also sits down with each patient when they register to go through the consent form. People with MS seem really motivated, so they are very helpful. MS research participants benefit from access to consortium's database for interdisciplinary research.

- Dr. LaRocca pointed out that it is much more than the incentives; these are highly motivated centers. Dr. Kasarskis added that a similar attempt had been made with ALS, but his perspective was that it had not worked because the academic payoff was not sufficient to motivate people to spend their time to complete the report. Basically, they

spent a great deal of uncompensated time, but there was no academic attribution back to them when the data were reported. Dr. Teter responded that those in the Consortium are authored and it is required by policy that every investigator and coordinator be acknowledged as well. Another important benefit of this database is the research results and dissemination of the information. The challenge, and one reason they hired a full-time coordinator, is that the 17 sites are extremely active. It is a major challenge to keep the system up and running on many fronts, and they are running in the red.

- Dr. Sorenson asked to what extent they were collecting longitudinal data. Dr. Teter replied that they are going through a logical tracking process to reduce missing data and track clinical follow-up and therefore, have successfully collected a hefty percentage of longitudinal data. Data collection has also been very successful because of how motivated MS patients are.

- It was noted that the issue of confidentiality is extremely confusing to patients / subjects, especially with consent that can continue on and on. Despite all of the guarantees made, as well as HIPAA protections, it is not clear how the patients / subjects know if they do or do not have confidentiality. Dr. Teter responded that in her experience, people were very willing to cooperate. People who are volunteering to go into the database are much more open. She has queried some of the nurse practitioners in Buffalo who explain that although HIPAA slows down their work, they have said that they do not believe there will be any problems with the patients / subjects if their information is shared with CDC and would be willing to consent.

- It was noted that sometimes minority populations seem to be very untrustworthy because their sense is that they continue to be used for research without getting anything out of it. Thus, it may have been a much greater challenge to obtain follow-up information in that population. Dr. Pentz pointed out that Grady is almost entirely a Black, under-served population, but they found no difference in their willingness to have information sent. In fact, they find no difference in any population with respect to helping with cancer.

Pilot Projects and Data Acquisition Update / Open Discussion — February 7, 2007

ALS Update

Kevin Horton, MSPH
Epidemiologist, Division of Health Studies
Agency for Toxic Substances and Disease Registry

Kevin Horton updated those present on the pilot projects and data acquisition. He reported that ATSDR has funded three pilot projects: Emory University, South Carolina, and the Mayo Clinic. This is a 2-year project which began in 2006 and will end in 2008.

For the past two to three months, ATSDR has been updating the data abstraction form. They first reviewed several ALS forms that have been used by various agencies around the country and pooled those together to develop a data abstraction form with which ATSDR is happy, as are the partners who are working with these forms now. The data abstraction form is a living document in that changes continue to be made to it, although they have reached a point where they are all fairly satisfied. The three partners are actually abstracting data from various databases utilizing the form. Along with the data abstraction form, ATSDR has developed an ACCESS database for the partners to use to abstract data, given that some states indicated they would rather input the data directly into the database. The ACCESS database is identical to the hardcopy data form.

With respect to the data sources, ATSDR has contacted the VA which has provided them with national data for these respective sites, which they now have in house. The statistician is currently going through the VA data looking at the layout. CMS data has been more of a challenge. ATSDR was told that the CMS data should reach them within the next few days. As with the VA data, the statisticians plan to review it and then send it out to the partners. He was not sure whether ATSDR will send CMS data with the VA data or separately, but they hope to get both the VA and CMS data out to the partners within the next month or so.

In conclusion, Mr. Horton thanked all of the partners and stressed that ATSDR had established a good relationship with them and he thought they were making good progress.

MS Update

Oleg Muravov, MD, PhD
Medical Epidemiologist
Surveillance and Registries Branch
Division of Health Studies
Agency for Toxic Substances and Disease Registry

Dr. Muravov reported that ATSDR requested and received data from VA for both MS and ALS in an effort to be cost-effective. They also received data from the National MS Society and are awaiting CMS data on Medicaid / Medicare. Their two pilots are two-year projects. New York is provided data by neurologists, so ATSDR hopes to conduct more analysis on this.

Open Discussion

- Dr. LaRocca said what he did not hear during the earlier presentations were any trials and tribulations from ATSDR about how any of what was reported earlier in the morning applied to the pilot studies.

- Dr. Kaye responded that as part of her consultation, she prepared all of the data packages for ATSDR for CMS and the VA. They had this discussion ahead of time because every institution views a request differently and the rules say that she can do

that. CMS actually has no mechanism for a public health request. The only mechanism is a research mechanism and there is a group at the University of Minnesota who assists in filling out forms, but it is from a research perspective. Hence, they had to pretend that they were conducting research because it must go through this process. The form is extensive so it took Dr. Kaye approximately 80 hours to complete. A major component is the security protocol. Mayo Clinic had to tell her their computer security protocol because she had to include ATSDR / CDC's protocol for protecting data as well as anyone else's protocol who will be touching the data. Gathering and putting together all of that information was time-consuming because it is extremely detailed (e.g., whether the computer is in a locked building, if there is a guard at the building, whether there is key card access, how often the passwords are changed, the construction of the passwords, et cetera). Dr. Kaye quipped that she had received a message from CMS stating, "We'd like you to tell us how our new security procedures are affecting your data" even though she has yet to receive any data. It turns out that CMS has a new procedure and policy for encryption of data, so ATSDR has no idea when these data show up whether they will even be able to un-encrypt it. It seems that the new procedure CMS is trying to work through is part of the hold-up in ATSDR receiving the data. It is not clear whether there will be additional constraints on ATSDR. CMS knows about and has approved the release of portions of these data to Mayo, Emory, and South Carolina but it is not clear whether there will be restrictions on security to release the data. Although the VA only tells people about the research mechanism, there is a public health mechanism for obtaining data. The public health road took six months to find, but once ATSDR found it, it only took two weeks to receive the data. VA does honor public health activity permitted release if provided with appropriate authorization. While ATSDR does have the VA data, it is in seven or so files and is not user-friendly.

- Dr. Kasarskis requested that Dr. Kaye further elaborate upon which "secret office" in the VA responds to public health activity requests.

- Dr. Kaye replied that it is the Privacy Officer, Stephanie Putt, who is in Florida. She is the Privacy Officer for the entire Veteran's Health Administration. ATSDR also requested pension and compensation data, but they do not have that data so she must seek it elsewhere in the VA. She will continue to pursue pension and compensation data from the VA because in some ways, that data is better than even the clinical data because patients have already been through the board, which has certified that they do have X disease. This information must be obtained from the Veterans Benefits Administration. All of the releases were requested with the idea that at this point, for the pilots, nobody will be contacted that is in the database. This is made very clear in these requests. They can be amended later to permit that, but it is another set of hurdles.

- Dr. Teter reiterated that New York is working with 17 sites and was hoping to come away with templates to go to each site and state what they want to do and what they need to obtain from each site. They expected to actually be working with the datasets doing matching and comparisons by summer. Although, in the last couple of months some IRBs at some of the sites have been extremely difficult, so this could slow them down to some extent. A major issue has regarded security of the data when it all comes

together. It does go in with initials. Over three years ago, the data were not with this data management company they are now using. It then involved Social Security Numbers, so they will have to deal with stripping those from older records. They are also doing a lot of quality control within the databases themselves, making sure fields give them the information they want, doing some logical checks, and making sure that the data are really useable.

- Dr. Sowell asked all of the pilot sites to discuss what type of data security they have set up and what issues they anticipated having with data security.

- Dr. Sorenson responded that Mayo's IRB covers all of the patients they will be seeing. They keep and maintain a database already for all ALS patients they see and maintain it, so they will probably turn around their portion of this very quickly once they receive the data from ATSDR. Every patient who presents at the institution signs a sheet that asks whether their medical records can be used for research as long as their confidentiality is protected. At Mayo the affirmative response rate is about 99.8% of patients, so they already have access to most of the records of everybody ever seen at Mayo. Therefore, they do not have to go back to individuals for further consent. However, anytime they start to populate any type of surveillance database that includes identifying information, they must obtain direct consent from each individual. This issue will arise beyond the pilot and actually creating the database. The Mayo Clinic database includes both patients who are there for a one-time visit with whom the relationship is not on-going because these patients return to their home physicians, as well as patients who have an on-going relationship with the Mayo Clinic. To go back to contact people, they would require IRB approval and there are several steps to this process: Individuals are sent a letter ahead of time to notify them that they will be called; they are given two weeks to respond regarding whether they would like to be called; et cetera. They cannot simply pick up the phone and call these people, and there is a rationale for doing this. Nevertheless, it is all workable. It is just a matter of going through the steps.

- Dr. Tyrell indicated that ORS has a locked building where data are housed. No one is allowed to enter except through the backside where the conference room is. Anyone entering main areas must be escorted. Computer access has multiple levels of security with different firewalls, security, and tracking devices in place where they track people and what they see on their computers. They have stringent controls on what people access even inside. When they receive data, they strip it and put it through the unique identifier process, and the unique identifier is put onto the rest of the data with the identifier stripped off. Identifiers are stored off site and require three different authorizations from three different levels to get the identifiers put back on. They have been vetted a couple of times by outside agencies and have been found to be in compliance with all of the HIPAA security guidelines.

- Dr. Sowell noted that because ORS puts their data through the unique identifier program, they would have to conduct backwards tracking once people in whom they were interested were selected.

- Dr. Tyrell replied that this process is relatively easy. They just have to complete another form which three people must sign off on to show that it is for a legitimate use.

- Because South Carolina has data from a variety of sources, Dr. Cwik wondered whether they would have to go back to those for additional consent or if their data agreements cover all potential uses.

- Dr. Tyrell responded that for CMS and the State Health Plan, the review process for them to use the data includes the Privacy Board approval. The in-patient, ambulatory surgery, home health, and other data are required to be reported to them by law. They have other supporting information about how they can use that data. ORS has to go through the Data Oversight Council, who has to give them approval, which is much like the Privacy Board approval. For the ALS / MS project, she had to go through about seven organizations to get various levels of privacy external to them, and then within their own organization she will have to obtain permission to link the data back to them.

- Dr. Schmidt asked whether the goal of the pilot projects was to get a list of people who have been diagnosed with MS or ALS in these local areas.

- Dr. Kaye responded that the goal was to evaluate what datasets are the best.

- Dr. Schmidt wondered whether any thought had been giving to staying away from names or unique identifiers when the data are combined in the first place, because it is a huge risk not only to the people, but also to the agencies contributing the data. That is, is there thought toward identification of the data at the local sites and encrypting that so it is still unique, but it cannot be traced back to the person who it represents.

- Dr. Sowell responded that one of the problems with doing something like that is that these are relatively rare diseases. Therefore, if they keep enough detail to be useful, they run the potential risk of being able to identify individuals even if there are no names or SSNs. Having only year and month of birth, location where they were diagnosed, and the fact that they have one of these diseases, for certain communities down to the county level, that will be enough to identify someone. HIPAA is very restrictive on that. This is a situation where, for the data to be useful, protected information must be included.

- Dr. Schmidt clarified that she was talking about encrypting the data when sending it from one location to another. Rather than sending straight text, they would all encrypt the data based on the same algorithm so that they could compare the results, but anybody who happened to get their hands on the data could not understand it.

- Dr. Sowell responded that the encryption issue is somewhat different from the privacy issue. There is a security issue. ATSDR is encouraging everybody to use encryption for data transfer. That is reasonable protection for transferring data. Data security can be complicated because at CDC, if data go onto a mainframe system or into the CDC network, the data number disappears. Some data agreements require that data be

destroyed after a certain point. In those situations, they are limited to only having data on individual computers—generally only on one computer. However, if something happens to that one computer, there is no back—up. There are several issues in terms of how protected the data are on the computer, whether there is any redundancy in the storage system, if redundancy is even allowed, et cetera.

- Dr. Tyrell replied that many of the review boards she goes through are asking for the exact name and address where offsite data is stored and whether that storage location knows the HIPAA rules for security.

- Dr. Sowell noted that there is a requirement in many places that anyone who has access to these data for computer security purposes must have taken appropriate training and must only be using the data on specified devices that have been approved by the privacy group.

- Dr. Schmidt inquired as to whether there was a way to get around that issue all together by never releasing identifiable data by creating a unique identifier.

- Dr. Tyrell responded that there is not because by definition HIPAA states that even random numbers constitute a unique identifier.

- Dr. Sowell added that replacing names and SSNs with random identification numbers and encryption does not prevent data from being identified. Other information could allow that individual to be identified. Confidentiality means more than just stripping off names and SSNs—it means making sure that if any of the data elements, or any combination of data elements would allow somebody to be identified, the people who have access to the data must be appropriate. An example of where data identification could have occurred is that one part of CDC conducts a survey called the National Health and Nutrition Examination Surveys (NHANES). NHANES surveys people around the U.S. and collects a great deal of demographic information, lifestyle information, physical measurements, blood, medical tests, et cetera. About 10 to 15 years ago, a large minority / ethnic family was involved in NHANES. Although names and identifiers were stripped in the commonly released data, the fact that it contained information on family size, geographic region, and ethnicity allowed all members of that family to be identified because the family size was large enough that it was a unique situation. That is when the NHANES group became very tight with whom they would share any data. Although she did not know the exact plan for what data would be collected for the ALS / MS surveillance system, the minimum information that would be useful would be some sort of indicators of age, geographic location, race / ethnicity, gender, the fact that they have one of these conditions, and probably the date when first diagnosed. If geographic region is only broken down by state, this will probably be okay. However, if there are five cases of MS or ALS in one state annually, it will be easy to identify those.

- Dr. Kaye pointed out that the tricky thing about HIPAA is that they clearly articulate 18 items they consider to be protected health information and include a clause that says, “or anything else that that could identify you.”

- Dr. Pentz added that there is also a clause that addresses having a statistician review it and work out the probabilities of identification.

- It was Dr. Sorenson's impression from their discussions earlier that they can create the surveillance database, including the identifying information, under the auspices of public health as long as it is only used for surveillance. The issue arises with respect to that database if someone wants to conduct research using information from it. If the researcher has IRB approval and oversight, they can obtain access to that information, including the identifying information, but for which the IRB may require further consent from individual subjects in the database.

- Dr. Kaye responded that the major issue regards how this is interpreted, which is left to the covered entity. VA has agreed that this is a public health activity and they are willing to allow it. CMS says that it is research, but they are willing to give a waiver of authorization. Yet, someone else says it is research and they will not give a waiver of authorization.

- Dr. Sorenson said that unless they can get it established as a public health initiative, they will never get it populated because they will run into this issue repeatedly. Otherwise, they will need explicit consent from each patient who provides identifying information. Speaking from his experience, he said he could not imagine any IRB in his institution approving the release of identifying information for research to anyone outside that institution without the subjects' explicit written consent. He stressed that if they approached this project under the auspices of research, there would be huge hurdles for everyone who wanted to put any information in.

- Dr. Tyrell replied that South Carolina has worked through these issues and will be able to populate it, although there this has all been approached as a research project. Whether consent would have to be obtained from each individual included in the database with identifying information would depend upon what other state laws overlay this. There are federal laws that apply to Medicaid data that are used at the state level. It is not as simple as just getting HIPAA and IRB approval. For a statewide collection, they must overlay programmatic and state laws and regulations on top of what they are doing to make them all fit together. She agreed that each location would face hurdles, and acknowledged that this is a problem that CDC will face when they are dealing with 50 + organizations in order to populate a national surveillance system. It is doable, but it will not be easy and cannot be done with a template.

- Dr. Kaye concurred that it would be nice to deal with as few entities as possible, so the idea with the pilots is to figure out what the fewest number of entities is that they can use and be accurate. For the pilot projects, ATSDR is giving identifiers to the pilots, but they are giving back de-identified datasets that basically say: Person 1, Person 2, Person 3, Person 4 . . . , which datasets they were in, and perhaps some information about age—whatever they can give without the person being identifiable. It will be an inclusive list so

that they will know how many people were in CMS who did not show up at the Mayo Clinic, or the VA, et cetera.

- Dr. Muravov said he thought the issue of encryptions was applicable to sending and storing data. When they do matching, they want to have as many identifiers as possible, so everything must be available to them. VA sent ATSDR a CD with a single zip file, password protected. They emailed him the password, which was a military level password to open the zip file, which included about eight files with different formats. It is not user-friendly. At this point, they do not know what kind of CMS data they will receive.

- Dr. Nelson requested further information about the National Multiple Sclerosis Society's contribution, as well as the potential for contributions from other patient service organizations and whether they perceived any barriers to organizations providing this information.

- Dr. LaRocca responded that the National Multiple Sclerosis Society has a database, which is really more of a mailing list of about 340,000 members, of which perhaps 300,000 actually exist. They provided this to ATSDR for matching purposes. His understanding is that segments of that will be provided to the pilot partners in the same way as the VA and CMS data to do the matching. They have a data use agreement with ATSDR about how these data can be used. With respect to distinguishing between who is a patient and who is not, people are coded. Part of the problem with that type of database is that there are errors in the coding, which they have taken into consideration in other studies in the past, so they now have an idea of the level of miscoding. They have been working the last few years to clean that up, although it is not as clean or sophisticated a database as others. However, what it lacks in terms of sophistication it somewhat makes up for in terms of its breadth. The Multiple Sclerosis Society is not a covered entity, so they are not subject to HIPAA and they have used the database in the past for a number of funded projects. When they fund a project to an extramural source, it always goes through an IRB. They also use their mailing list to conduct their own intramural marketing research for their organization, in which case they do not go through an IRB because this is an internal function.

- Dr. Sorenson indicated that the Mayo Clinic is also working with the Minnesota Chapter of the ALS Association to obtain information for the entire state. They are still working on the type of data they will receive to complement the data they have.

- Dr. Tyrell reported that South Carolina is going to meet with the local ALS Association on Friday. Part of the problem with South Carolina is that it was served by North Carolina for a long time, so the split is relatively recent. Therefore, it is not clear how much of South Carolina is still in North Carolina. These are the issues they will be discussing during their meeting. There are three clinics: Georgia, North Carolina, and South Carolina.

- Dr. Nelson inquired as to whether the Muscular Dystrophy Association (MDA) or the ALS Association (ALSA) planned to provide any national lists.

- Dr. Kaye said it was her understanding that ALSA does not have a national list.

- Dr. Cwik responded that MDA basically has a mailing list and does not collect data of any sort. They also have some coding problems, which are more complex because they are dealing with about 40 different diseases. They are not a covered entity, but they do sign business associates agreements with a number of institutions because they fund 225 clinics across the country. She was not sure how that potentially could impact sharing of that kind of information.

- With regard to ALS, Sharon Usher said that Emory has a verbal agreement for sharing information. For the MDA they have the medical directors of local chapters: Medical College of Georgia, Emory, and two other chapters. These are through the clinics, not coming through the MDA offices.

- Dr. Kaye said the difference with ALS is that they will have to make individual agreements with the partners that will affect their population versus with the National Multiple Sclerosis Society where it is one group. However, then there is the other issue of miscoding, so ATSDR received additional data to help ensure that they were not mailing to anyone who is diseased, for example. They were all coded that they had MS and were not a family member or just an interested party.

- Dr. Kasarskis inquired as to whether there was anything being built at any level of CDC, public health, or government entity, to determine what the perceptions of the public would be, how much individual privacy people would give up and under what circumstances, in order to facilitate a broader national public health research infrastructure. Hearing what South Carolina's level of security is, as a patient he would be inclined to be included so they could learn something about X. Less than that and people would be concerned. ALS patients are highly motivated to understand what caused their disease and the same is probably true with MS patients. They could pick five diseases at random and would hear similar sentiments. What they really want to do with this ALS / MS surveillance effort is research in order to get at some of the global questions which they cannot sort out with an N of 1.

- Dr. Garbe responded that he was not aware of anything like that; however, CDC is so fragmented now, it is easy for one part of the agency to do something that nobody else in the agency knows anything about. He said he heard a distinction between the activities of surveillance, where the personal identifying information is not that critical compared to building a research database. Building a research database is not something that CDC is typically going to be doing. The scope of in-depth research databases is more of an NIH province. There may be overlap in approaches that NIH grantees are using, which are very comparable to activities CDC is engaged in with its state health department partnerships. But the focus of NIH-funded projects would be the research questions; whereas, the focus that CDC has with states is more enumeration and counting. Where identifiers are useful is so that they do not double count, or where there are so few people with a condition in a particular geographic area that they cannot

report that information as in the NHANES example. The National Center for Health Statistics (NCHS) has an N of 5 rule; that is, when they stratify data and report, if the cell size is 5 or fewer, they do not report the number because with a little effort, someone could figure out who the people are in the cell.

- Dr. Pentz said she had exactly the same question as Dr. Kasarskis when Professor Hodge said people would not join clinical trials and they would not be supportive if there were not privacy protections. However, her own experience with patients is that the concern is not there. She thinks they need the research.

- Dr. Kasarskis acknowledged that identity theft is a hot topic, that people are suspicious of government agencies, that there is a natural road block that people do not want to be told what to do, and that this is a very bad U.S. climate in which to talk about community good. Holding hands and singing "Kumbayah" is just not going to happen very much; however, there may be a certain threshold at which people would agree to do this for the common good of health maintenance or disease prevention.

- Dr. Culpepper said he knew of one paper from about three or four years ago from North Carolina where they were collecting cancer reporting information directly from physicians. Then someone decided that perhaps they should survey the patients to determine what they thought about this. The results of the survey indicated that only 3% to 4% of patients, when asked how they felt, were infuriated and requested that their names be removed as they would have declined if they had been asked at the outset. However, the vast majority agreed to be included. About 60% percent said they would rather be contacted directly than to have the physician make that decision. He offered to send the article to Dr. Kasarskis.

- Dr. Kasarskis indicated that in the VA ALS registry there is parallel universe of DNA collection, which has multiple layers of security that only the VA can do. It is extraordinarily user-friendly, meaning that if someone is assigned into this registry to be enumerated in this database, then they are asked a second time if they would make a one-time blood donation for the DNA bank. This is different than the NINDS somewhat because these are not immortalized cells, so this is strictly in a bank of DNA that is isolated. The VA has made it even easier in the sense that they send a nurse to the individuals' homes to draw the blood, so individuals have no excuse not to participate other than they do not want to. The positive response rate is approximately 90%. They had a paper accepted recently, with a lead author out of Durham, which discusses who refuses. Even under that circumstance, among military personnel, minorities come through. That is, there is a low refusal rate, but it is clearly distinguished from Caucasians. Even though the "skids were greased," they still had refusals and there were differences about who opted out and who did not. Obviously, they are always in the category of good enough versus perfect. To some degree, a 97% population agreement rate is beyond good enough.

- Dr. Cwik inquired as to whether patient communities are aware that this MS / ALS initiative is underway and that the pilot study has started, or if there was a reason to let

them know or not to let them know at this point. Dr. Bruijn said she had expressed that same question to Kevin Horton, who said he could work with his team to put out a brief commentary that they could all use on their websites. Until now, things were still in process, but it seems like a good time, with the public interest and the advocacy efforts that ALSA has been making as well, to put something together. Dr. Kaye indicated that Dr. Muravov could develop something for MS as well, but the information may have to go through a clearance mechanism. Dr. Horton agreed that ATSDR could develop a summary paragraph with general information about the pilot studies, the ultimate goal of a national registry, et cetera.

- Dr. Kasarskis asked Dr. Kaye to give a synopsis of whether ATSDR thought this project was where they anticipated it to be at this point.

- Dr. Kaye replied that realistically they were about where she would have expected, or maybe even a little ahead of schedule, given the meeting last March. At least in principle they have gotten two of the largest groups to give them information (e.g., VA and CMS). While they have not actually received the CMS data, they soon will. They were able to fund five pilot project groups, who have been working their way through laws, policies, and procedures in their institutions to the point that it looks like once the data are available and ATSDR is able to give it to the pilot groups, the pilot groups will be ready to use it. She did not see any reason why the pilots would not be completed when expected in 2008. It sounded like some groups may even be ahead of schedule, so ATSDR was not saying they should wait two years if they did not have to. Not knowing how long the approvals would take from states, universities, or government, ATSDR had to build in a year to get the preliminary work done.

- Dr. Nelson inquired as to what geographic region the Emory group is covering and what their data sources are, the timeframe for case ascertainment, and whether death certificates would be used in all three locations. She thought it would be nice for all of the sites to know, if they were to rely on death certificates alone, what percentage of cases are captured and if it varies from state to state.

- Dr. Kaye replied that Emory is covering the entire State of Georgia and their data sources are VA, CMS, the Georgia ALSA chapter, neurologists' offices, and the Medical College of Georgia. With respect to case ascertainment, Dr. Kaye indicated that the national datasets requested are for 2001 through 2005. These are the prevalence cases because someone may have just appeared in 2001, or they may have been there for several years and are still there in 2001. That is one of the questions: How many years of data are needed to actually find a person? This is probably a bigger question for MS than for ALS because once an ALS individual is identified, they stay in until they die; whereas, MS individuals may be jumping in and out.

- Regarding death certificates, Dr. Sorenson indicated that they will not attempt to overlap the death certificates with the pilot data. They do routinely use death certificates when trying to ascertain survival status for ALS patients. Death certificates are a matter of public record, so permission is not needed to use them.

- Dr. Tyrell indicated that South Carolina is already looking at death certificate data and how many cases would have been missed if they had used death certificate data or other data and vice versa. They are excited about this because they have gotten interesting preliminary results.

- Dr. Muravov reminded everyone that the VA office they have been dealing with does not have any data on pensions and benefits or in-patient out-patient versus pharmacy information. They did collect patient information from the late nineties, but they have collected pharmacy only starting in 2002, so they realize that their dates of 2001 through 2005 will not be complete. Dr. Kaye added that the reason this is important for the VA dataset is that someone can be approved to receive pharmacy benefits from the VA, but may receive their medical care from outside the VA system. There is a significant financial benefit from receiving pharmacy benefits from a VA. So, by using pharmacy data, they will find some additional patients that would be missed with only in-patient / out-patient data.

- Dr. Kasarskis responded that this varies by VA facility. Although the national office has put in print that the VA does not want to posture themselves as a pharmacy, this is skirted. For example, somebody with MS who has a private neurologist presents at the VA for their medication and then returns to their private neurologist. However, this is actively discouraged by the VA. Presumably, with this information, ATSDR will have a true positive at least of an N of 1, but they will not be able to attribute that identification to a VA healthcare system, only to a VA pharmacy.

- Dr. Culpepper added that in 2002, the VA mandated that anybody receiving prescriptions through the VA must be seen by a VA provider. What they have noticed in the MS datasets is that the number of people who have only been identified through pharmacy data has dwindled. For 2005, this was only 22 individuals. He also noted that MS and ALS drugs are non-formulary and require specific, authorized individuals at each facility to prescribe. At his facility they have two individuals who are MS specialist neurologists who have authority to make that prescription, while routine neurologists cannot do so. Therefore, patients must come through that MS clinic to be captured and verified that the medications are indicated for those individuals because such high costs are involved.

- Dr. Kasarskis said that depending on how poor the patient is financially, they may be pressured to get all of their care through the VA just so they can obtain their medication. The pharmacy tab in the VA system represents a major cost, which is why they have a centralized formulary—in order to get economy of scale. This is closely scrutinized and the rules change weekly. He pointed out that the beauty of the electronic record is that someone can try to dodge the system, but it takes only a key stroke to find that a patient is not enrolled in VA primary care, they have never had an encounter with any VA primary care provider, and they are only visiting the pharmacy. The power of health information—there is no escape from that within the VA system.

Wrap-Up and Adjourn

February 7, 2007

In closing, Dr. Kaye thanked everyone for their participation and contributions. She indicated that they would receive a report of the workshop in approximately the two to three month range. With no further business posed, she officially adjourned the meeting.

End of Report

♦♦♦

Dr. Pentz pointed out that academic medicine differs from other settings in various ways. Part of this has to do with scale. CDC has seven IRBs, while Emory University has five. True about all IRBs is that they all have their own characteristics depending upon the membership, which causes numerous issues. Emory's IRBs function as HIPAA authorization boards; that is, if someone wants a HIPAA waiver, they would seek that from the IRB. Emory also has the resources to formalize most requirements. Each of the following links leads to a form that an investigator can fill out, so no investigator can make any excuses for not knowing how to complete the forms if they can figure out which forms they need:

HIPAA Forms

HIPAA Assurance Regarding Disclosure of a Decedent's PHI for Research Purposes
HIPAA Authorization Form for Use and Disclosure of Protected Health Information for Research Purposes\
HIPAA Authorization for Use/Disclosure of Protected Health Information by Emory University to a Third Party
HIPAA Authorization for Use/Disclosure of Protected Health Information From a Third Party to Emory University
HIPAA Authorization for Use/Disclosure of Psychotherapy Notes by Emory University to a Third Party
HIPAA Business Associate Agreement
HIPAA Business Associate Confidentiality Agreement
HIPAA Business Associate Security Agreement
HIPAA Consent and Authorization for Protected Health Information to be Included in a Research Database
HIPAA Data Use Agreement
HIPAA Illustrations of Situations Requiring/Not Requiring Authorization
HIPAA Listing of Typical Business Associates
HIPAA Log to Track Disclosures of PHI
HIPAA Patient Authorization for Use and Disclosure of Protected Health Information
HIPAA Patient Complaint Form
HIPAA Patient Consent for Use and Disclosure of Protected Health Information for Treatment, Payment and Health Care Operations Purposes
HIPAA Patient Consent to Means of Communication
HIPAA Patient Denial Letter
HIPAA Privacy Policy Training Checklist
HIPAA Privacy Representative's Incident Event Log
HIPAA Receipt of Notice of Privacy Practices Written Acknowledgement Form
HIPAA Request for an Accounting of Certain Disclosures of Protected Health Information for Non-TPO Purposes
HIPAA Request for Correction/Amendment of Protected Health Information
HIPAA Request for Limitations and Restrictions of Protected Health Information
HIPAA Request to Inspect and Copy Protected Health Information
HIPAA Workforce Confidentiality Agreement

IRB HIPAA Forms

IRB: Combined Informed Consent/HIPAA Authorization
IRB: HIPAA Authorization Revocation Letter
IRB: HIPAA Stand-Alone Authorization Template
IRB: HIPAA Worksheet/Application for Waiver of Authorization

Emory is considered to have "deep pockets," so they do get sued. In one of the latest cases they have had, Emory employees were privately subcontracting with a public health agency to conduct research. They were using a reportable disease database, which is where they obtained their information. They were doing cold calling using an Emory phone bank, so when people received the call it said "Emory University" on their caller identification. One person saw "Emory University" on their phone who did not have the disease the investigators were calling about, had no idea why they were in the database, and subsequently sued Emory. Hence, the Emory lawyers are reasonable, but they are cautious.

HIPAA was expensive for Emory. Start-up included $463,000 for outside counsel for HIPAA analysis, 75% of an in-house counsel's time for a year, and it continues to cost major dollars for the work that they are doing. Other on-going costs include continuous risk analysis, updating of all electronic software, and monitoring against confidentiality threats.

There are confidentiality threats. A laptop with Emory patient PHI was stolen from a private contractor. Emory sent out a letter to all patients explaining how to find out whether there has been any breech in their confidentiality. In a similar situation with the University of Pennsylvania, the university paid for all credit checking. However, Emory did not do this. In another incident, a subcontractor lost a USB pin with Emory patient information.

Another major difference between an academic medical center and other settings, particularly public health, is that the focus of the academic center and of the IRBs (even though they have an excellent school of public health and they live right down the road from CDC) at Emory is on the individual patient. It is very difficult for them to see public health kinds of issues. Personal autonomy is the bedrock principle, even to the extent that it gets in the way of a lot of other issues. Medicine is based on the physician-patient dyad. The core ethical principle is respect for individual autonomy. That is, public health ethics is not the coin of the realm in academic medicine. Even with all of the public health that surrounds them, this is why Emory's IRBs and researchers will be focused on individual patients.

Also different in an academic versus other settings is that the culture of academic medicine is hierarchical with tenured professors at the top. There is no doubt that the hierarchical, tenured system is a medieval caste system. Caps and gowns became the official academic dress proclaimed in 1321 AD, and this has not changed at all. What that means practically is that in hierarchical systems, it is easier to get a project approved by working laterally (e.g., professor to professor, physician to physician, PhD to PhD, epidemiologist to epidemiologist).

Academics can be arcane and they consider themselves experts—sometimes a panel of experts is not needed, yet IRBs are full of panels of experts. For example, a sociologist criticizes an oncology protocol as too invasive when it actually is just beyond the standard of care. Or an oncologist criticizes a social science questionnaire as too sensitive. Sometimes, even though they are experts in their field, they have no clue about what the standard of practice is in other fields. Nevertheless, the times are changing. Academic institutions are becoming more entrepreneurial. It is amazing how much money one can make in academic medicine currently. Tenure is not as important anymore as fame and fortune. For example, Dr. Pentz just reviewed a case of an assistant professor who has never written a successful NIH grant, but who runs a small biotech company where he is making multi-millions and has eight employees.

Emory has a full-time HIPAA expert who makes all of the decisions. Dr. Pentz visited with her to explain the discussions in the March ALS / MS workshop. The Emory HIPAA expert declared it to be research and said that it has to follow the rules as they stand. Therefore, what is needed to use Emory patient information in a database for a retrospective study is that data must be de-identified or include a limited data set (dates, city, state, zip). For a prospective study, they must have consent and HIPAA authorization. Either must have IRB approval. That said, because they are academic, if a cogent, well-argued analytical case, Dr. Pentz's experience is that the IRB and their HIPAA authority will respond to it because they are moved by concepts. One of her jobs at Emory is when a person has an excellent idea, but which is a little "squiggly" on the regulations, she puts together the case to show that it should move forward as a public health activity. They often "win the day." Therefore, it is not impossible to move this registry forward, but they may have to make a compelling argument that it is not research.

Discussion Points:

- Dr. Kasarskis thought this got down to a point of law because it sounded as though, if Congress decided legally that ALS and MS are public health problems which need to be solved with a public health approach, the proposed system presumably would be removed from some of these considerations.

- Using cancer as a model, Dr. Kaye pointed out that when Congress decided there should be a war on cancer, one way to do this was through a cancer registry. Congress awarded funding to CDC to start a cancer registry, and there was a requirement that to obtain funding, each state had to make cancer a reportable disease. Many of the state laws do include fines and penalties for people who do not report and some have exercised that authority on occasion. Although Congress might say ALS / MS are reportable and states have to do it, that delegation has historically been given to the states. With infectious diseases it has been easier to make this argument than with chronic diseases.

- Dr. Kasarskis said during the March workshop, they concluded that this may not be a viable approach, but he wanted to understand some of the principles that would underlie what would be brought out as something broader than just the patient / physician contact and exchange of information.

- Dr. Kaye replied that she helped write the applications to places like CMS to gain access to identifiable data. The fact that someone has become interested, from a public health perspective, in obtaining information on incidence and prevalence is part of the argument for why they should have access to this information. While this does not require the owners of the data to give the information, it does make them think more kindly upon the application for it.

- Professor Hodge added that Congress really cannot push states around, but they can attach it to funding. The important aspect from the HIPAA Privacy Rule perspective is that at the state level, they do not have to line item detail that they may now collect MS or ALS data via some surveillance practice. That is not required by the Privacy Rule. They simply have to show that the acquisition of these data are in the interest of protecting the public's health and that it is done by a public health agency or a contractor of a public health agency. While a statutory regulation might make it easier to obtain the data, they could launch this surveillance system at the state level now with only consensus that this is a public health objective to which many states believe it is essential to contribute.

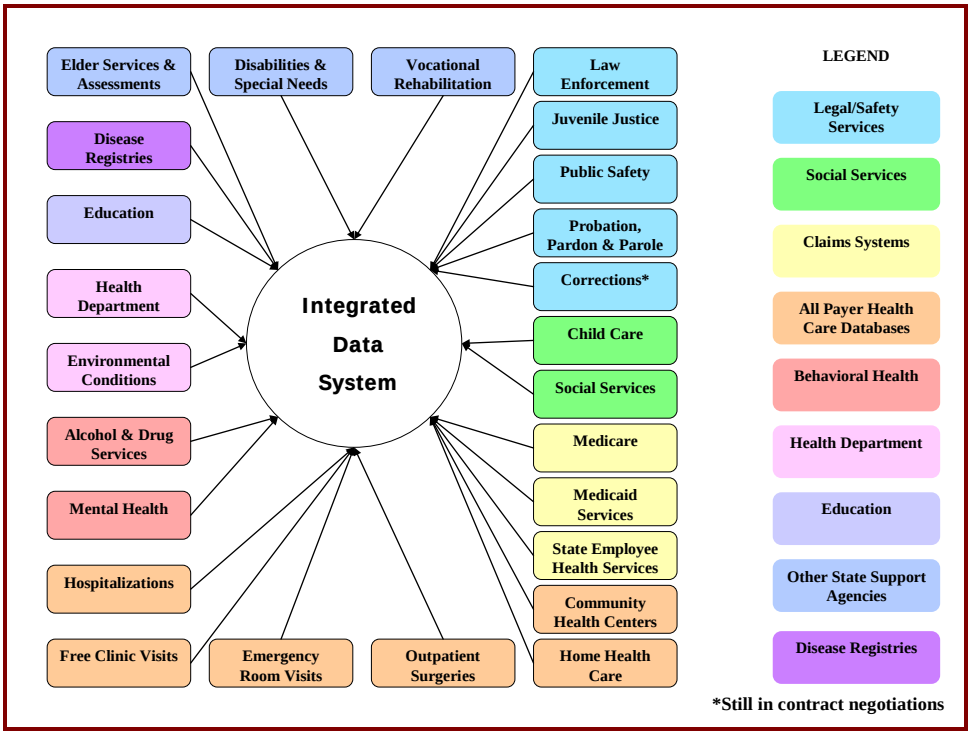
IRB and HIPAA Issues from a State Perspective — February 7, 2007

Mary Tyrell, PhD
South Carolina Budget and Control Board
Office of Research and Statistics

Dr. Tyrell stressed that her message to them was that not only are there differences with HIPAA and IRBs, but every state has different laws. When considering the conduct of a surveillance project, this means dealing with 50+ methods of data collection for a variety of diseases. Three of the most common forms of data collection include: Public Health Agencies, Other State Data Agencies, and Hospital Associations. Models for data sharing include administrative, statutory, and contractual / voluntary. She explained that her office is not a public health organization; they are strictly an office of research and statistics. They have no regulatory / statutory authority to implement, regulate, license, or in any way do anything for the systems in South Carolina. Their mission is merely to conduct data research and other functions for other state agencies, universities, and other interested parties. With respect to population-based surveillance, in a lot of the states the hospital associations collect the in-patient and emergency department (ED) data. There are other non-profit organizations collecting data as well. Complicating all of these different systems that are collecting data is that there are different models for data sharing. Some agencies,

hospitals, associations, and other entities can have the authority within their organizations to decide to share or not share data. Some of this authority is statutory, which is true in South Carolina. Dr. Tyrell must work through a legislatively mandated committee to make determinations about data sharing. If someone requesting data does not like the decision the committee makes, it can go to an administrative law judge, circuit court, and all the way up if desired. The bottom line is that no matter what type of agency or what model of data sharing is utilized, all must adhere to HIPAA and IRB as they pertain to the individual organizations.

The following illustrates the dataset to which the Office of Research and Statistics (ORS) has access:



Not only must the ORS comply with HIPAA, but also they must comply with FERPA and numerous other rules and regulations. They have the ability to link and track anyone across all of these data sets—it is extremely powerful. They have the ability to look at not only what happens when someone presents for ALS, but also if they are covered by Medicaid services, there is a record of all of the physicians' data, all the tests they have received, et cetera. That is the good news. The bad news is that there is a different method to access every single data base in this system.

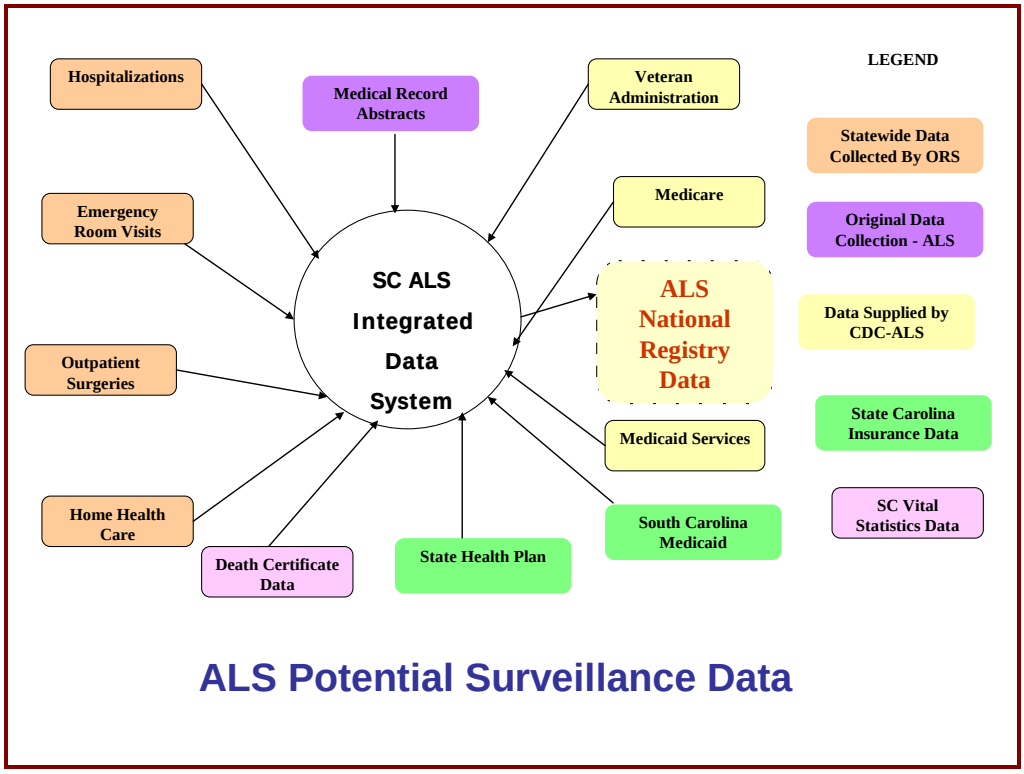
Dr. Tyrell reiterated that she cannot allow anybody to use the data without going through their formal access process. Nevertheless, South Carolina's uniqueness is that there is one entry point to multiple data sets (ORS). For a surveillance project, for example, CDC / ATSDR would contract with ORS only. The ORS staff coordinates all access to data bases. Part of the reason they choose to do that is because over the years they have developed a very good relationship with most of their data partners. Every state agency in South Carolina gives ORS virtually every data set they have, so they must be very judicious in guarding and sharing data to ensure that all of their actions are truly in the best interest of the citizens of South Carolina.

Part of what they do is administrative. South Carolina has Medicaid and a state health plan. Teachers in any school in the state, firefighters anywhere in the state, almost every county health department employee, and others are considered to be state employees. Therefore, South Carolina has more state employees than any other state, because they are covered by the state health insurance plan. Therefore, when those two data sets are linked, all healthcare encounter information is on record for 1.25 million people or a quarter of the population of South Carolina. So, the state health plan is an administrative process.

State laws guide the use of these data sets as well. This is where state laws overlay HIPAA, FERPA, et cetera for in-patient, ED, and out-patient data. There are federal programs such as Medicaid that guide that, and there are contractual limitations. With respect to medical record abstraction, because they can link and track, they can do all sorts of individual clinical data, et cetera. Researchers can provide their data and ORS can link and track it with appropriate accesses, they can de-identify it, and can give the researcher back not only their data, but also whatever other data they have requested. CDC / ATSDR receives one, unduplicated, linked dataset. There are some types of access that are really a combination of multiple levels, such as vital statistics. On occasion not only do they have to get a vital statistics approval, but also IRB and other types of approval. Therefore, it is imperative to understand that access takes time for any project.

One of the benefits of the ORS data sets is that recipients can get an unduplicated, linked data set across all of the various data sets. For example, specific to the ALS data set, Dr. Tyrell can link and unduplicate anyone who has had an ALS diagnosis or encounter anywhere in the state across five years. They can look at some who were diagnosed after the first year, pre- and post-encounters, what they came into before, what they came into after, whether they have died and if so at what point, et cetera. The beauty of all of that is ORS can combine this, de-identify it to satisfy IRBs and HIPAA, and provide it back to the person requesting it.

The following illustration depicts the South Carolina ALS project:



South Carolina will be using hospital in-patient, ED visits, out patient surgeries, and home health care. ORS has all of this information for anybody in South Carolina who was served by any South Carolina facility. They are going to add to this the death certificate, state health plan, and South Carolina Medicaid data. Although Dr. Tyrell acknowledged that Medicaid data are being obtained at the federal level, she requested the South Carolina Medicaid data because she can get access to every database that Medicaid has and all of the different types of information, including extensive eligibility information. People on Medicaid in South Carolina tend to come and go for a variety of reasons, so this helps them to look at standing: When were they eligible? One unfortunate person in their study so far has been in ORS's hospital, ED, outpatient surgery, home health care, state health plan, and Medicaid data over five years. The ability to look at this information in this manner is very powerful, especially with respect to incidence and prevalence rates, treated prevalence rates, et cetera.

South Carolina has successfully moved through all of the access issues. Their goal now is to generate the integrated database, de-identify it, and supply it back to CDC / ATSDR for this project. ORS is also adding medical records data, which means they must communicate with private providers. From the state perspective, this means that they may have to go through an IRB. ORS cannot directly collect medical records data; they must contract with the public health organization which has to collect the data, although they

cannot see the names and addresses. They have been working on a method to do this where the public health organization can see names and addresses only when the abstractor gets to the institution, physician, hospital, or wherever it is they are going to do the abstracting. Prior to that, any information must be de-identified because of some of the rules that were set up under South Carolina law, which have nothing to do with HIPAA or IRB. This adds a level of even more complexity and issues they must deal with, including additional time, which will delay the deliverables to CDC / ATSDR.

In terms of how all of this relates to computer enhancements and electronic advances that have been made, Dr. Tyrell shared several examples of what South Carolina is doing with this type of data. They have developed an electronic personal health record for all Medicaid patients in South Carolina, which is in the process of being rolled out currently to every private provider in the state. They do plan to track individual authorizations for all Medicaid patients (over 900,000 individuals), including rejections. Also, someone presenting in the ED can give authorization and the hospital can access all healthcare services they have received in any of the datasets participating in that combined collection of information.

They also have the Client Information Management System where they have linked every person receiving services in all of South Carolina's social services and state agencies. This system can be rolled out at the county level to the actual clinical or social worker, who can see every encounter that a person has had with any state agency, including the date and extensive information about what has happened to that person. This is also done by consent of the individual patient. They also have the right once they consent to retract that consent. This is all done in accordance with HIPAA security regulations. For anyone who accesses any of these entries, every key stroke is tracked and kept for six years.

With respect to what this all means, HIPAA does allow for the use of limited data sets, which is basically ORS's philosophy and is what they try to do with all of their researchers. South Carolina state law for ORS, the hospital ED data, in-patient, out-patient, et cetera pre-empts HIPAA because not only can ORS not identify a person, but also they cannot identify a physician or health care facility. While with appropriate authorization she might be able to share a hospital name with CDC, CDC cannot share it with anyone else. For patient identifiable data HIPAA requires an IRB; however, state laws have different requirements. Dr. Tyrell noted that while someone may tell her they have an IRB, she still may have to apply to seven or eight other entities requesting information. An IRB at their state level, and in other states, may make it go faster but they will still have to go through all of the access issues. She had one research project that had to go through 65 IRBs because nobody could agree. With that in mind, her message was that while they have the ability to conduct incredible research in South Carolina, all of it takes time. What used to take two to three years will now probably take four to five years simply because they must go through all of the approval processes.

Discussion Points:

- Dr. LaRocca asked what basic strategy is used by ORS to de-duplicate such a wide variety of records. Dr. Tyrell replied that they have a system called Unique ID Process, which takes multiple information from many data sets and uses them as gold standard IDs. There are other ways they can link back to eligibility files and they have them all put into a specific algorithm they use, although she said that for security and confidentiality purposes she could not disclose the details. Currently, their false positives are running about one in one million records. They have a goal to cut that at least by 10 times. They have someone working on this now and due to a couple of improvements, they believe they will be able to cut this down to about one in 10 million. They have over 100 million records in the data set, which continues to grow.

- Dr. Kasarskis inquired as to how they were able to obtain VA data. Dr. Tyrell responded that they receive Department of Defense (DoD) data who also receives data from ORS, and they receive VA data. However, the limitation is that they cannot use those data for specialized projects, for example the ALS project. This is one of the caveats on which they are working. South Carolina has extensive military and it is critical to what they do.

- Dr. Cwik acknowledged that clearly South Carolina has been very proactive on this collection of data bases, which is incredibly powerful, and she wondered how South Carolina compared to other states.

- Dr. Tyrell replied that there is no other state in the United States that can do the breadth and depth of data that South Carolina can do. There are about 44 states which collect some type of in-patient and ED data and 38 states that collect additional types of data. South Carolina's uniqueness is that they have added the social services, juvenile justice, and criminal data. She stressed that they must move beyond just health care data because so much what they do has implications in the social services, economics, and employment sectors. Dr. Kaye added that they are not aware of any other state that has a data set like South Carolina.

IRB and HIPAA Issues from a Private Registry Perspective

February 7, 2007

Barbara Teter, MPH, CHES, PhD
Director of Clinical Research and Development
New York State Multiple Sclerosis Consortium
The Jacobs Neurological Institute

Dr. Teter reported on the New York State Multiple Sclerosis Consortium (NYSMSC), which was established in 1994 to develop a durable database of demographic and clinical data to promote MS research and enhance patient care. Membership includes 17 sites in New York State, 27 investigators (MDs and PhDs), and 30 research or data coordinators (NPs, RNs, RAs, MSWs, and PhDs). The database includes 8,500 + registered MS patients and 14,000 + follow-up records. At the point of patient enrollment, it is disclosed that this information is being collected for research in compliance with IRB human subjects consent and HIPAA requirements.

The NYSMSC is governed by an Executive-Finance Committee, and data utilization is governed by a Scientific Review Committee. The NYSMSC is administered by an Executive Director, and a Director of Clinical Research and Development. Procedures and policy revisions require a membership quorum. With respect to policy, it is important to understand security and quality control. Official policies cover mandatory site activity, consortium membership requests for data forms, consortium membership submission of complete data forms, internal NYSMSC data requests, data ownership, external data requests and research collaborations, as well as a policy regarding NYSMSC revenues, and publications based on NYSMSC data. Consortium members can request their own data or data for all other sites.

In terms of data management and security, the database is physically housed at Uniform Data System for Medical Rehabilitation (UDSMR). They are a reputable location with their own privacy policies and a disaster recovery plan. UDSMR complies with all government PHI rules. Data are stored on a Microsoft SQL server.

Pertaining to data collection for the registry, the patient completes the first 24 questions (of 40 question sets) regarding demographic factors (date of birth, gender, race), reproductive factors, education, living environment, employment, family history (MS and other illnesses), and a self-assessment of function. Clinicians (MDs NPs) complete 15 question sets, which include MS symptoms (onset and current), MS types, characteristics of attacks, remissions, physiological characteristics (CSF and MRI), functional scores (characteristics), psychological characteristics, and DMT (disease modifying therapies). The NYSMSC database does include identifiers (patient initials [non-variable], date of birth, address, gender, and ethnicity). It does not include name, Social Security Number (SSN) or partial SSN. They understand that the ATSDR surveillance database is contingent on the value of pilot project and that ATSDR would be the keeper of a minimal database, including PHI.

In terms of the language on the consent form, membership sites comply with the IRBs of their individual institutions utilizing a consortium protocol. The title of the project is: The Establishment of a Patient Registry and Initiation of Related Projects of the New York State Multiple Sclerosis Consortium. An excerpt from the consent form describing the project reads as follows, "The purpose of the Consortium is to obtain a more accurate understanding of MS in New York State in terms of prevalence, demographics, functional capabilities, …. and treatment regimes, etc."

Consent includes information on site of study unique to each membership site; principal investigators' names and contact information; a statement of research; introduction and background; procedures; risks and discomforts; potential benefits; confidentiality, reimbursement, study costs, voluntary participation; alternatives to participation; new findings; authorization for use and disclosure of identifiable health information for research purposes; and patient signatures for voluntary consent to participate. Included with consent is an authorization for use and disclosure of identifiable health information for research purposes. Subjects are told the following: "Your health information may be shared with others outside the research group for purposes directly related to conduct of this research study or as required by law, including but not limited to NYSMSC investigators and designees; UDSMR; individuals responsible for general oversight and compliance activities; and government agencies with authority over the research including HHS, FDA, NIH, OHRP

The next step is expected to be participation in the national surveillance system. The NYSMSC database does not include patient names; however, unique identifiers can be linked to names and would require each consortium site to provide a name. Linking and reporting would require a waiver of consent and a waiver of authorization. For NYSMSC to report names with other identifiers to a national surveillance system, further consent would need to be obtained from each of the participants.

Discussion Points:

- Dr. Kasarskis inquired as to who pays for the NYSMSC database and how practitioners are compensated for collecting the data. Dr. Teter replied that New York State provided the funding for the initial set-up. The Consortium is receiving a small amount of funding, but is actively pursuing additional funding. Regarding practitioner compensation, they reimburse $30 per registration form and $30 for each follow-up form. The fees are the same across the state. Once they locate additional funding, they plan to increase the follow-up fee. The target for that compensation is to retain someone in a physician's office to ensure that the physician is completing the information. That person also sits down with each patient when they register to go through the consent form. People with MS seem really motivated, so they are very helpful. MS research participants benefit from access to consortium's database for interdisciplinary research.

- Dr. LaRocca pointed out that it is much more than the incentives; these are highly motivated centers. Dr. Kasarskis added that a similar attempt had been made with ALS, but his perspective was that it had not worked because the academic payoff was not sufficient to motivate people to spend their time to complete the report. Basically, they

spent a great deal of uncompensated time, but there was no academic attribution back to them when the data were reported. Dr. Teter responded that those in the Consortium are authored and it is required by policy that every investigator and coordinator be acknowledged as well. Another important benefit of this database is the research results and dissemination of the information. The challenge, and one reason they hired a full-time coordinator, is that the 17 sites are extremely active. It is a major challenge to keep the system up and running on many fronts, and they are running in the red.

- Dr. Sorenson asked to what extent they were collecting longitudinal data. Dr. Teter replied that they are going through a logical tracking process to reduce missing data and track clinical follow-up and therefore, have successfully collected a hefty percentage of longitudinal data. Data collection has also been very successful because of how motivated MS patients are.

- It was noted that the issue of confidentiality is extremely confusing to patients / subjects, especially with consent that can continue on and on. Despite all of the guarantees made, as well as HIPAA protections, it is not clear how the patients / subjects know if they do or do not have confidentiality. Dr. Teter responded that in her experience, people were very willing to cooperate. People who are volunteering to go into the database are much more open. She has queried some of the nurse practitioners in Buffalo who explain that although HIPAA slows down their work, they have said that they do not believe there will be any problems with the patients / subjects if their information is shared with CDC and would be willing to consent.

- It was noted that sometimes minority populations seem to be very untrustworthy because their sense is that they continue to be used for research without getting anything out of it. Thus, it may have been a much greater challenge to obtain follow-up information in that population. Dr. Pentz pointed out that Grady is almost entirely a Black, under-served population, but they found no difference in their willingness to have information sent. In fact, they find no difference in any population with respect to helping with cancer.

Pilot Projects and Data Acquisition Update / Open Discussion — February 7, 2007

ALS Update

Kevin Horton, MSPH
Epidemiologist, Division of Health Studies
Agency for Toxic Substances and Disease Registry

Kevin Horton updated those present on the pilot projects and data acquisition. He reported that ATSDR has funded three pilot projects: Emory University, South Carolina, and the Mayo Clinic. This is a 2-year project which began in 2006 and will end in 2008.

For the past two to three months, ATSDR has been updating the data abstraction form. They first reviewed several ALS forms that have been used by various agencies around the country and pooled those together to develop a data abstraction form with which ATSDR is happy, as are the partners who are working with these forms now. The data abstraction form is a living document in that changes continue to be made to it, although they have reached a point where they are all fairly satisfied. The three partners are actually abstracting data from various databases utilizing the form. Along with the data abstraction form, ATSDR has developed an ACCESS database for the partners to use to abstract data, given that some states indicated they would rather input the data directly into the database. The ACCESS database is identical to the hardcopy data form.

With respect to the data sources, ATSDR has contacted the VA which has provided them with national data for these respective sites, which they now have in house. The statistician is currently going through the VA data looking at the layout. CMS data has been more of a challenge. ATSDR was told that the CMS data should reach them within the next few days. As with the VA data, the statisticians plan to review it and then send it out to the partners. He was not sure whether ATSDR will send CMS data with the VA data or separately, but they hope to get both the VA and CMS data out to the partners within the next month or so.

In conclusion, Mr. Horton thanked all of the partners and stressed that ATSDR had established a good relationship with them and he thought they were making good progress.

MS Update

Oleg Muravov, MD, PhD
Medical Epidemiologist
Surveillance and Registries Branch
Division of Health Studies
Agency for Toxic Substances and Disease Registry

Dr. Muravov reported that ATSDR requested and received data from VA for both MS and ALS in an effort to be cost-effective. They also received data from the National MS Society and are awaiting CMS data on Medicaid / Medicare. Their two pilots are two-year projects. New York is provided data by neurologists, so ATSDR hopes to conduct more analysis on this.

Open Discussion

- Dr. LaRocca said what he did not hear during the earlier presentations were any trials and tribulations from ATSDR about how any of what was reported earlier in the morning applied to the pilot studies.

- Dr. Kaye responded that as part of her consultation, she prepared all of the data packages for ATSDR for CMS and the VA. They had this discussion ahead of time because every institution views a request differently and the rules say that she can do

that. CMS actually has no mechanism for a public health request. The only mechanism is a research mechanism and there is a group at the University of Minnesota who assists in filling out forms, but it is from a research perspective. Hence, they had to pretend that they were conducting research because it must go through this process. The form is extensive so it took Dr. Kaye approximately 80 hours to complete. A major component is the security protocol. Mayo Clinic had to tell her their computer security protocol because she had to include ATSDR / CDC's protocol for protecting data as well as anyone else's protocol who will be touching the data. Gathering and putting together all of that information was time-consuming because it is extremely detailed (e.g., whether the computer is in a locked building, if there is a guard at the building, whether there is key card access, how often the passwords are changed, the construction of the passwords, et cetera). Dr. Kaye quipped that she had received a message from CMS stating, "We'd like you to tell us how our new security procedures are affecting your data" even though she has yet to receive any data. It turns out that CMS has a new procedure and policy for encryption of data, so ATSDR has no idea when these data show up whether they will even be able to un-encrypt it. It seems that the new procedure CMS is trying to work through is part of the hold-up in ATSDR receiving the data. It is not clear whether there will be additional constraints on ATSDR. CMS knows about and has approved the release of portions of these data to Mayo, Emory, and South Carolina but it is not clear whether there will be restrictions on security to release the data. Although the VA only tells people about the research mechanism, there is a public health mechanism for obtaining data. The public health road took six months to find, but once ATSDR found it, it only took two weeks to receive the data. VA does honor public health activity permitted release if provided with appropriate authorization. While ATSDR does have the VA data, it is in seven or so files and is not user-friendly.

- Dr. Kasarskis requested that Dr. Kaye further elaborate upon which "secret office" in the VA responds to public health activity requests.

- Dr. Kaye replied that it is the Privacy Officer, Stephanie Putt, who is in Florida. She is the Privacy Officer for the entire Veteran's Health Administration. ATSDR also requested pension and compensation data, but they do not have that data so she must seek it elsewhere in the VA. She will continue to pursue pension and compensation data from the VA because in some ways, that data is better than even the clinical data because patients have already been through the board, which has certified that they do have X disease. This information must be obtained from the Veterans Benefits Administration. All of the releases were requested with the idea that at this point, for the pilots, nobody will be contacted that is in the database. This is made very clear in these requests. They can be amended later to permit that, but it is another set of hurdles.

- Dr. Teter reiterated that New York is working with 17 sites and was hoping to come away with templates to go to each site and state what they want to do and what they need to obtain from each site. They expected to actually be working with the datasets doing matching and comparisons by summer. Although, in the last couple of months some IRBs at some of the sites have been extremely difficult, so this could slow them down to some extent. A major issue has regarded security of the data when it all comes

together. It does go in with initials. Over three years ago, the data were not with this data management company they are now using. It then involved Social Security Numbers, so they will have to deal with stripping those from older records. They are also doing a lot of quality control within the databases themselves, making sure fields give them the information they want, doing some logical checks, and making sure that the data are really useable.

- Dr. Sowell asked all of the pilot sites to discuss what type of data security they have set up and what issues they anticipated having with data security.

- Dr. Sorenson responded that Mayo's IRB covers all of the patients they will be seeing. They keep and maintain a database already for all ALS patients they see and maintain it, so they will probably turn around their portion of this very quickly once they receive the data from ATSDR. Every patient who presents at the institution signs a sheet that asks whether their medical records can be used for research as long as their confidentiality is protected. At Mayo the affirmative response rate is about 99.8% of patients, so they already have access to most of the records of everybody ever seen at Mayo. Therefore, they do not have to go back to individuals for further consent. However, anytime they start to populate any type of surveillance database that includes identifying information, they must obtain direct consent from each individual. This issue will arise beyond the pilot and actually creating the database. The Mayo Clinic database includes both patients who are there for a one-time visit with whom the relationship is not on-going because these patients return to their home physicians, as well as patients who have an on-going relationship with the Mayo Clinic. To go back to contact people, they would require IRB approval and there are several steps to this process: Individuals are sent a letter ahead of time to notify them that they will be called; they are given two weeks to respond regarding whether they would like to be called; et cetera. They cannot simply pick up the phone and call these people, and there is a rationale for doing this. Nevertheless, it is all workable. It is just a matter of going through the steps.

- Dr. Tyrell indicated that ORS has a locked building where data are housed. No one is allowed to enter except through the backside where the conference room is. Anyone entering main areas must be escorted. Computer access has multiple levels of security with different firewalls, security, and tracking devices in place where they track people and what they see on their computers. They have stringent controls on what people access even inside. When they receive data, they strip it and put it through the unique identifier process, and the unique identifier is put onto the rest of the data with the identifier stripped off. Identifiers are stored off site and require three different authorizations from three different levels to get the identifiers put back on. They have been vetted a couple of times by outside agencies and have been found to be in compliance with all of the HIPAA security guidelines.

- Dr. Sowell noted that because ORS puts their data through the unique identifier program, they would have to conduct backwards tracking once people in whom they were interested were selected.

- Dr. Tyrell replied that this process is relatively easy. They just have to complete another form which three people must sign off on to show that it is for a legitimate use.

- Because South Carolina has data from a variety of sources, Dr. Cwik wondered whether they would have to go back to those for additional consent or if their data agreements cover all potential uses.

- Dr. Tyrell responded that for CMS and the State Health Plan, the review process for them to use the data includes the Privacy Board approval. The in-patient, ambulatory surgery, home health, and other data are required to be reported to them by law. They have other supporting information about how they can use that data. ORS has to go through the Data Oversight Council, who has to give them approval, which is much like the Privacy Board approval. For the ALS / MS project, she had to go through about seven organizations to get various levels of privacy external to them, and then within their own organization she will have to obtain permission to link the data back to them.

- Dr. Schmidt asked whether the goal of the pilot projects was to get a list of people who have been diagnosed with MS or ALS in these local areas.

- Dr. Kaye responded that the goal was to evaluate what datasets are the best.

- Dr. Schmidt wondered whether any thought had been giving to staying away from names or unique identifiers when the data are combined in the first place, because it is a huge risk not only to the people, but also to the agencies contributing the data. That is, is there thought toward identification of the data at the local sites and encrypting that so it is still unique, but it cannot be traced back to the person who it represents.

- Dr. Sowell responded that one of the problems with doing something like that is that these are relatively rare diseases. Therefore, if they keep enough detail to be useful, they run the potential risk of being able to identify individuals even if there are no names or SSNs. Having only year and month of birth, location where they were diagnosed, and the fact that they have one of these diseases, for certain communities down to the county level, that will be enough to identify someone. HIPAA is very restrictive on that. This is a situation where, for the data to be useful, protected information must be included.

- Dr. Schmidt clarified that she was talking about encrypting the data when sending it from one location to another. Rather than sending straight text, they would all encrypt the data based on the same algorithm so that they could compare the results, but anybody who happened to get their hands on the data could not understand it.

- Dr. Sowell responded that the encryption issue is somewhat different from the privacy issue. There is a security issue. ATSDR is encouraging everybody to use encryption for data transfer. That is reasonable protection for transferring data. Data security can be complicated because at CDC, if data go onto a mainframe system or into the CDC network, the data number disappears. Some data agreements require that data be

destroyed after a certain point. In those situations, they are limited to only having data on individual computers—generally only on one computer. However, if something happens to that one computer, there is no back—up. There are several issues in terms of how protected the data are on the computer, whether there is any redundancy in the storage system, if redundancy is even allowed, et cetera.

- Dr. Tyrell replied that many of the review boards she goes through are asking for the exact name and address where offsite data is stored and whether that storage location knows the HIPAA rules for security.

- Dr. Sowell noted that there is a requirement in many places that anyone who has access to these data for computer security purposes must have taken appropriate training and must only be using the data on specified devices that have been approved by the privacy group.

- Dr. Schmidt inquired as to whether there was a way to get around that issue all together by never releasing identifiable data by creating a unique identifier.

- Dr. Tyrell responded that there is not because by definition HIPAA states that even random numbers constitute a unique identifier.

- Dr. Sowell added that replacing names and SSNs with random identification numbers and encryption does not prevent data from being identified. Other information could allow that individual to be identified. Confidentiality means more than just stripping off names and SSNs—it means making sure that if any of the data elements, or any combination of data elements would allow somebody to be identified, the people who have access to the data must be appropriate. An example of where data identification could have occurred is that one part of CDC conducts a survey called the National Health and Nutrition Examination Surveys (NHANES). NHANES surveys people around the U.S. and collects a great deal of demographic information, lifestyle information, physical measurements, blood, medical tests, et cetera. About 10 to 15 years ago, a large minority / ethnic family was involved in NHANES. Although names and identifiers were stripped in the commonly released data, the fact that it contained information on family size, geographic region, and ethnicity allowed all members of that family to be identified because the family size was large enough that it was a unique situation. That is when the NHANES group became very tight with whom they would share any data. Although she did not know the exact plan for what data would be collected for the ALS / MS surveillance system, the minimum information that would be useful would be some sort of indicators of age, geographic location, race / ethnicity, gender, the fact that they have one of these conditions, and probably the date when first diagnosed. If geographic region is only broken down by state, this will probably be okay. However, if there are five cases of MS or ALS in one state annually, it will be easy to identify those.

- Dr. Kaye pointed out that the tricky thing about HIPAA is that they clearly articulate 18 items they consider to be protected health information and include a clause that says, “or anything else that that could identify you.”

- Dr. Pentz added that there is also a clause that addresses having a statistician review it and work out the probabilities of identification.

- It was Dr. Sorenson's impression from their discussions earlier that they can create the surveillance database, including the identifying information, under the auspices of public health as long as it is only used for surveillance. The issue arises with respect to that database if someone wants to conduct research using information from it. If the researcher has IRB approval and oversight, they can obtain access to that information, including the identifying information, but for which the IRB may require further consent from individual subjects in the database.

- Dr. Kaye responded that the major issue regards how this is interpreted, which is left to the covered entity. VA has agreed that this is a public health activity and they are willing to allow it. CMS says that it is research, but they are willing to give a waiver of authorization. Yet, someone else says it is research and they will not give a waiver of authorization.

- Dr. Sorenson said that unless they can get it established as a public health initiative, they will never get it populated because they will run into this issue repeatedly. Otherwise, they will need explicit consent from each patient who provides identifying information. Speaking from his experience, he said he could not imagine any IRB in his institution approving the release of identifying information for research to anyone outside that institution without the subjects' explicit written consent. He stressed that if they approached this project under the auspices of research, there would be huge hurdles for everyone who wanted to put any information in.

- Dr. Tyrell replied that South Carolina has worked through these issues and will be able to populate it, although there this has all been approached as a research project. Whether consent would have to be obtained from each individual included in the database with identifying information would depend upon what other state laws overlay this. There are federal laws that apply to Medicaid data that are used at the state level. It is not as simple as just getting HIPAA and IRB approval. For a statewide collection, they must overlay programmatic and state laws and regulations on top of what they are doing to make them all fit together. She agreed that each location would face hurdles, and acknowledged that this is a problem that CDC will face when they are dealing with 50 + organizations in order to populate a national surveillance system. It is doable, but it will not be easy and cannot be done with a template.

- Dr. Kaye concurred that it would be nice to deal with as few entities as possible, so the idea with the pilots is to figure out what the fewest number of entities is that they can use and be accurate. For the pilot projects, ATSDR is giving identifiers to the pilots, but they are giving back de-identified datasets that basically say: Person 1, Person 2, Person 3, Person 4 . . . , which datasets they were in, and perhaps some information about age—whatever they can give without the person being identifiable. It will be an inclusive list so

that they will know how many people were in CMS who did not show up at the Mayo Clinic, or the VA, et cetera.

- Dr. Muravov said he thought the issue of encryptions was applicable to sending and storing data. When they do matching, they want to have as many identifiers as possible, so everything must be available to them. VA sent ATSDR a CD with a single zip file, password protected. They emailed him the password, which was a military level password to open the zip file, which included about eight files with different formats. It is not user-friendly. At this point, they do not know what kind of CMS data they will receive.

- Dr. Nelson requested further information about the National Multiple Sclerosis Society's contribution, as well as the potential for contributions from other patient service organizations and whether they perceived any barriers to organizations providing this information.

- Dr. LaRocca responded that the National Multiple Sclerosis Society has a database, which is really more of a mailing list of about 340,000 members, of which perhaps 300,000 actually exist. They provided this to ATSDR for matching purposes. His understanding is that segments of that will be provided to the pilot partners in the same way as the VA and CMS data to do the matching. They have a data use agreement with ATSDR about how these data can be used. With respect to distinguishing between who is a patient and who is not, people are coded. Part of the problem with that type of database is that there are errors in the coding, which they have taken into consideration in other studies in the past, so they now have an idea of the level of miscoding. They have been working the last few years to clean that up, although it is not as clean or sophisticated a database as others. However, what it lacks in terms of sophistication it somewhat makes up for in terms of its breadth. The Multiple Sclerosis Society is not a covered entity, so they are not subject to HIPAA and they have used the database in the past for a number of funded projects. When they fund a project to an extramural source, it always goes through an IRB. They also use their mailing list to conduct their own intramural marketing research for their organization, in which case they do not go through an IRB because this is an internal function.

- Dr. Sorenson indicated that the Mayo Clinic is also working with the Minnesota Chapter of the ALS Association to obtain information for the entire state. They are still working on the type of data they will receive to complement the data they have.

- Dr. Tyrell reported that South Carolina is going to meet with the local ALS Association on Friday. Part of the problem with South Carolina is that it was served by North Carolina for a long time, so the split is relatively recent. Therefore, it is not clear how much of South Carolina is still in North Carolina. These are the issues they will be discussing during their meeting. There are three clinics: Georgia, North Carolina, and South Carolina.

- Dr. Nelson inquired as to whether the Muscular Dystrophy Association (MDA) or the ALS Association (ALSA) planned to provide any national lists.

- Dr. Kaye said it was her understanding that ALSA does not have a national list.

- Dr. Cwik responded that MDA basically has a mailing list and does not collect data of any sort. They also have some coding problems, which are more complex because they are dealing with about 40 different diseases. They are not a covered entity, but they do sign business associates agreements with a number of institutions because they fund 225 clinics across the country. She was not sure how that potentially could impact sharing of that kind of information.

- With regard to ALS, Sharon Usher said that Emory has a verbal agreement for sharing information. For the MDA they have the medical directors of local chapters: Medical College of Georgia, Emory, and two other chapters. These are through the clinics, not coming through the MDA offices.

- Dr. Kaye said the difference with ALS is that they will have to make individual agreements with the partners that will affect their population versus with the National Multiple Sclerosis Society where it is one group. However, then there is the other issue of miscoding, so ATSDR received additional data to help ensure that they were not mailing to anyone who is diseased, for example. They were all coded that they had MS and were not a family member or just an interested party.

- Dr. Kasarskis inquired as to whether there was anything being built at any level of CDC, public health, or government entity, to determine what the perceptions of the public would be, how much individual privacy people would give up and under what circumstances, in order to facilitate a broader national public health research infrastructure. Hearing what South Carolina's level of security is, as a patient he would be inclined to be included so they could learn something about X. Less than that and people would be concerned. ALS patients are highly motivated to understand what caused their disease and the same is probably true with MS patients. They could pick five diseases at random and would hear similar sentiments. What they really want to do with this ALS / MS surveillance effort is research in order to get at some of the global questions which they cannot sort out with an N of 1.

- Dr. Garbe responded that he was not aware of anything like that; however, CDC is so fragmented now, it is easy for one part of the agency to do something that nobody else in the agency knows anything about. He said he heard a distinction between the activities of surveillance, where the personal identifying information is not that critical compared to building a research database. Building a research database is not something that CDC is typically going to be doing. The scope of in-depth research databases is more of an NIH province. There may be overlap in approaches that NIH grantees are using, which are very comparable to activities CDC is engaged in with its state health department partnerships. But the focus of NIH-funded projects would be the research questions; whereas, the focus that CDC has with states is more enumeration and counting. Where identifiers are useful is so that they do not double count, or where there are so few people with a condition in a particular geographic area that they cannot

report that information as in the NHANES example. The National Center for Health Statistics (NCHS) has an N of 5 rule; that is, when they stratify data and report, if the cell size is 5 or fewer, they do not report the number because with a little effort, someone could figure out who the people are in the cell.

- Dr. Pentz said she had exactly the same question as Dr. Kasarskis when Professor Hodge said people would not join clinical trials and they would not be supportive if there were not privacy protections. However, her own experience with patients is that the concern is not there. She thinks they need the research.

- Dr. Kasarskis acknowledged that identity theft is a hot topic, that people are suspicious of government agencies, that there is a natural road block that people do not want to be told what to do, and that this is a very bad U.S. climate in which to talk about community good. Holding hands and singing "Kumbayah" is just not going to happen very much; however, there may be a certain threshold at which people would agree to do this for the common good of health maintenance or disease prevention.

- Dr. Culpepper said he knew of one paper from about three or four years ago from North Carolina where they were collecting cancer reporting information directly from physicians. Then someone decided that perhaps they should survey the patients to determine what they thought about this. The results of the survey indicated that only 3% to 4% of patients, when asked how they felt, were infuriated and requested that their names be removed as they would have declined if they had been asked at the outset. However, the vast majority agreed to be included. About 60% percent said they would rather be contacted directly than to have the physician make that decision. He offered to send the article to Dr. Kasarskis.

- Dr. Kasarskis indicated that in the VA ALS registry there is parallel universe of DNA collection, which has multiple layers of security that only the VA can do. It is extraordinarily user-friendly, meaning that if someone is assigned into this registry to be enumerated in this database, then they are asked a second time if they would make a one-time blood donation for the DNA bank. This is different than the NINDS somewhat because these are not immortalized cells, so this is strictly in a bank of DNA that is isolated. The VA has made it even easier in the sense that they send a nurse to the individuals' homes to draw the blood, so individuals have no excuse not to participate other than they do not want to. The positive response rate is approximately 90%. They had a paper accepted recently, with a lead author out of Durham, which discusses who refuses. Even under that circumstance, among military personnel, minorities come through. That is, there is a low refusal rate, but it is clearly distinguished from Caucasians. Even though the "skids were greased," they still had refusals and there were differences about who opted out and who did not. Obviously, they are always in the category of good enough versus perfect. To some degree, a 97% population agreement rate is beyond good enough.

- Dr. Cwik inquired as to whether patient communities are aware that this MS / ALS initiative is underway and that the pilot study has started, or if there was a reason to let

them know or not to let them know at this point. Dr. Bruijn said she had expressed that same question to Kevin Horton, who said he could work with his team to put out a brief commentary that they could all use on their websites. Until now, things were still in process, but it seems like a good time, with the public interest and the advocacy efforts that ALSA has been making as well, to put something together. Dr. Kaye indicated that Dr. Muravov could develop something for MS as well, but the information may have to go through a clearance mechanism. Dr. Horton agreed that ATSDR could develop a summary paragraph with general information about the pilot studies, the ultimate goal of a national registry, et cetera.

- Dr. Kasarskis asked Dr. Kaye to give a synopsis of whether ATSDR thought this project was where they anticipated it to be at this point.

- Dr. Kaye replied that realistically they were about where she would have expected, or maybe even a little ahead of schedule, given the meeting last March. At least in principle they have gotten two of the largest groups to give them information (e.g., VA and CMS). While they have not actually received the CMS data, they soon will. They were able to fund five pilot project groups, who have been working their way through laws, policies, and procedures in their institutions to the point that it looks like once the data are available and ATSDR is able to give it to the pilot groups, the pilot groups will be ready to use it. She did not see any reason why the pilots would not be completed when expected in 2008. It sounded like some groups may even be ahead of schedule, so ATSDR was not saying they should wait two years if they did not have to. Not knowing how long the approvals would take from states, universities, or government, ATSDR had to build in a year to get the preliminary work done.

- Dr. Nelson inquired as to what geographic region the Emory group is covering and what their data sources are, the timeframe for case ascertainment, and whether death certificates would be used in all three locations. She thought it would be nice for all of the sites to know, if they were to rely on death certificates alone, what percentage of cases are captured and if it varies from state to state.

- Dr. Kaye replied that Emory is covering the entire State of Georgia and their data sources are VA, CMS, the Georgia ALSA chapter, neurologists' offices, and the Medical College of Georgia. With respect to case ascertainment, Dr. Kaye indicated that the national datasets requested are for 2001 through 2005. These are the prevalence cases because someone may have just appeared in 2001, or they may have been there for several years and are still there in 2001. That is one of the questions: How many years of data are needed to actually find a person? This is probably a bigger question for MS than for ALS because once an ALS individual is identified, they stay in until they die; whereas, MS individuals may be jumping in and out.

- Regarding death certificates, Dr. Sorenson indicated that they will not attempt to overlap the death certificates with the pilot data. They do routinely use death certificates when trying to ascertain survival status for ALS patients. Death certificates are a matter of public record, so permission is not needed to use them.

- Dr. Tyrell indicated that South Carolina is already looking at death certificate data and how many cases would have been missed if they had used death certificate data or other data and vice versa. They are excited about this because they have gotten interesting preliminary results.

- Dr. Muravov reminded everyone that the VA office they have been dealing with does not have any data on pensions and benefits or in-patient out-patient versus pharmacy information. They did collect patient information from the late nineties, but they have collected pharmacy only starting in 2002, so they realize that their dates of 2001 through 2005 will not be complete. Dr. Kaye added that the reason this is important for the VA dataset is that someone can be approved to receive pharmacy benefits from the VA, but may receive their medical care from outside the VA system. There is a significant financial benefit from receiving pharmacy benefits from a VA. So, by using pharmacy data, they will find some additional patients that would be missed with only in-patient / out-patient data.

- Dr. Kasarskis responded that this varies by VA facility. Although the national office has put in print that the VA does not want to posture themselves as a pharmacy, this is skirted. For example, somebody with MS who has a private neurologist presents at the VA for their medication and then returns to their private neurologist. However, this is actively discouraged by the VA. Presumably, with this information, ATSDR will have a true positive at least of an N of 1, but they will not be able to attribute that identification to a VA healthcare system, only to a VA pharmacy.

- Dr. Culpepper added that in 2002, the VA mandated that anybody receiving prescriptions through the VA must be seen by a VA provider. What they have noticed in the MS datasets is that the number of people who have only been identified through pharmacy data has dwindled. For 2005, this was only 22 individuals. He also noted that MS and ALS drugs are non-formulary and require specific, authorized individuals at each facility to prescribe. At his facility they have two individuals who are MS specialist neurologists who have authority to make that prescription, while routine neurologists cannot do so. Therefore, patients must come through that MS clinic to be captured and verified that the medications are indicated for those individuals because such high costs are involved.

- Dr. Kasarskis said that depending on how poor the patient is financially, they may be pressured to get all of their care through the VA just so they can obtain their medication. The pharmacy tab in the VA system represents a major cost, which is why they have a centralized formulary—in order to get economy of scale. This is closely scrutinized and the rules change weekly. He pointed out that the beauty of the electronic record is that someone can try to dodge the system, but it takes only a key stroke to find that a patient is not enrolled in VA primary care, they have never had an encounter with any VA primary care provider, and they are only visiting the pharmacy. The power of health information—there is no escape from that within the VA system.

Wrap-Up and Adjourn

February 7, 2007

In closing, Dr. Kaye thanked everyone for their participation and contributions. She indicated that they would receive a report of the workshop in approximately the two to three month range. With no further business posed, she officially adjourned the meeting.

End of Report

♦♦♦

List of Invited Participants

February 7, 2007

Michael Benatar, MD
Neurologist
Emory Department of Neurology
Atlanta, GA

Lucie Bruijn, PhD
Science Director and Vice President
Amyotrophic Lateral Sclerosis Association
Calabasas Hills, CA

Sharon Campolucci, RN
Deputy Director, Division of Health Studies
Agency for Toxic Substances and Disease Registry
Atlanta, GA

William J. Culpepper II, MA
Baltimore Veterans Affairs Medical Center
Baltimore, MD

Valerie A. Cwik, MD
Medical Director
Muscular Dystrophy Association
Tucson, AZ 85718

Paul Garbe, DVM, MPH
Acting Chief
Air Pollution and Respiratory Health Branch
Division of Environmental Hazards and Health Effects
National Center for Environmental Health
Centers for Disease Control and Prevention
Atlanta, GA

Steve Gibson
Vice President, Government Relations & Public Affairs
Amyotrophic Lateral Sclerosis Association
Washington, DC

Carolyn Harris
Division of Health Studies
Agency for Toxic Substances and Disease Registry
Atlanta, GA

James G. Hodge, Jr.
Associate Professor
Johns Hopkins Bloomberg School of Public Health
Executive Director
Center for Law and the Public's Health
Core Faculty, Berman Bioethics Institute
Baltimore, MD

Kevin Horton, MSPH
Epidemiologist
Division of Health Studies
Agency for Toxic Substances and Disease Registry
Atlanta, GA

Vikas Kapil, DO, MPH, FACOEM
Chief, Surveillance and Registries Branch
Division of Health Studies
Agency for Toxic Substances and Disease Registry
Atlanta, GA

Edward J. Kasarskis, MD, PhD
Co-Principle Investigator
VA ALS Registry
VA Neurology Service
Lexington, KY

Mark Kashdan, JD
Office of the General Counsel
CDC/ATSDR Branch
Atlanta, GA

Wendy E. Kaye, PhD,
Senior Epidemiologist
McKing Consulting Corporation
Atlanta, GA

Annie Kennedy
Director, ALS Division
Muscular Dystrophy Association
Tucson, AZ

List of Invited Participants

February 7, 2007

Michael Benatar, MD
Neurologist
Emory Department of Neurology
Atlanta, GA

Lucie Bruijn, PhD
Science Director and Vice President
Amyotrophic Lateral Sclerosis Association
Calabasas Hills, CA

Sharon Campolucci, RN
Deputy Director, Division of Health Studies
Agency for Toxic Substances and Disease Registry
Atlanta, GA

William J. Culpepper II, MA
Baltimore Veterans Affairs Medical Center
Baltimore, MD

Valerie A. Cwik, MD
Medical Director
Muscular Dystrophy Association
Tucson, AZ 85718

Paul Garbe, DVM, MPH
Acting Chief
Air Pollution and Respiratory Health Branch
Division of Environmental Hazards and Health Effects
National Center for Environmental Health
Centers for Disease Control and Prevention
Atlanta, GA

Steve Gibson
Vice President, Government Relations & Public Affairs
Amyotrophic Lateral Sclerosis Association
Washington, DC

Carolyn Harris
Division of Health Studies
Agency for Toxic Substances and Disease Registry
Atlanta, GA

James G. Hodge, Jr.
Associate Professor
Johns Hopkins Bloomberg School of Public Health
Executive Director
Center for Law and the Public's Health
Core Faculty, Berman Bioethics Institute
Baltimore, MD

Kevin Horton, MSPH
Epidemiologist
Division of Health Studies
Agency for Toxic Substances and Disease Registry
Atlanta, GA

Vikas Kapil, DO, MPH, FACOEM
Chief, Surveillance and Registries Branch
Division of Health Studies
Agency for Toxic Substances and Disease Registry
Atlanta, GA

Edward J. Kasarskis, MD, PhD
Co-Principle Investigator
VA ALS Registry
VA Neurology Service
Lexington, KY

Mark Kashdan, JD
Office of the General Counsel
CDC/ATSDR Branch
Atlanta, GA

Wendy E. Kaye, PhD,
Senior Epidemiologist
McKing Consulting Corporation
Atlanta, GA

Annie Kennedy
Director, ALS Division
Muscular Dystrophy Association
Tucson, AZ

Nicolas G. LaRocca, PhD
Director, Health Care Delivery and Policy Research
National Multiple Sclerosis Society
New York, NY

Jennifer C. MacDonald, MPA
Public Health Analyst
Division of Health Studies
Agency for Toxic Substances and Disease Registry
Atlanta, GA

Jay Mandrekar, PhD
Statistician
Mayo Clinic
Rochester, MN

Sharon J. Matland, RN, MBA
Vice President, Patient Services
Amyotrophic Lateral Sclerosis Association
Calabasas Hills, CA

Oleg Muravov, MD, PhD
Medical Epidemiologist
Surveillance and Registries Branch
Division of Health Studies
Agency for Toxic Substances and Disease Registry
Atlanta, GA

Lorene Nelson, PhD
Associate Professor & Chief, Division of Epidemiology
Department of Health Research & Policy
Stanford University School of Medicine
Stanford, CA

Rebecca Pentz, PhD
Professor of Research Ethics,
Winship Cancer Institute
Emory University
Atlanta, GA

Julie Royer
Statistician
South Carolina Budget and Control Board
Office of Research and Statistics
Columbia, South Carolina

Jay Sapp, MS
Statistician
Division of Health Studies
Agency for Toxic Substances and Disease Registry
Atlanta, GA

Hollie Schmidt, MS, DS/MS
Vice President, Scientific Operations
Accelerated Cure Project for Multiple Sclerosis
Waltham, MA

James Sejvar, MD
Neuroepidemiologist
National Center for Infectious Diseases
Centers for Disease Control and Prevention
Atlanta, GA

Youn K. Shim, Ph.D.
Epidemiologist
Division of Health Studies
Agency for Toxic Substances and Disease Registry
Atlanta, GA

Judy Smith
Division of Health Studies
Agency for Toxic Substances and Disease Registry
Atlanta, GA

Eric Sorenson, MD
Neurologist
Mayo Clinic
Rochester, MN

Anne Sowell, PhD
Associate Director for Science
Division of Health Studies
Agency for Toxic Substances and Disease Registry
Atlanta, GA

David Thurman MD, MPH
Centers for Disease Control and Prevention
Atlanta, GA

Deborah Tress, JD
Principal Senior Attorney
Office of the General Counsel
CDC/ATSDR Branch
Atlanta, GA

Barbara Teter, MPH CHES, PhD
Director of Clinical Research and Development
NYS Multiple Sclerosis Consortium
Jacobs Neurological Institute
Buffalo, NY

Mary Tyrell, Ph.D.
South Carolina Budget and Control Board
Office of Research & Statistics
Columbia, SC

Susan Usher, RN
Research Nurse
Emory Department of Neurology
Woodruff Memorial Building
Atlanta, GA

G. David Williamson, PhD
Director, Division of Health Studies
Agency for Toxic Substances and Disease Registry
Atlanta, GA 30333