March 18, 2014

John W. Hounsell
Business and Industry Specialist
Office of Product and Program Management
National Technical Information Service
Department of Commerce
5301 Shawnee Road
Alexandria, VA 22312

Re: Certification Program for Access to the Death Master File

Dear Mr. Hounsell:

On behalf of The Society of Thoracic Surgeons (STS), the largest organization representing cardiothoracic surgeons in the United States and the world, I write to provide comments on the request for information pertaining to the Commerce Department’s certification program for access to the Death Master File (DMF). Founded in 1964, The Society of Thoracic Surgeons is an international not-for-profit organization representing more than 6,700 members located in 85 countries, who are dedicated to ensuring the best possible outcomes for surgeries of the heart, lung, and esophagus, as well as other surgical procedures within the chest.

The STS National Database was established in 1989 as an initiative for quality improvement and patient safety. The STS National Database has three components—Adult Cardiac, General Thoracic, and Congenital Heart Surgery. STS has also partnered with the American College of Cardiology (ACC) to create the STS/ACC TVT Registry, a data repository developed to track patient safety and real-world outcomes related to the transcatheter aortic valve replacement (TAVR) procedure. The TVT Registry has been approved by the Centers for Medicare and Medicaid Services (CMS) to meet the registry requirement outlined in the Medicare National Coverage Decision on TAVR.

The Duke Clinical Research Institute (DCRI) is the data warehouse and analysis center for the STS National Database. On behalf of STS, DCRI develops participant-specific reports that provide analysis of participants’ adult cardiac surgery outcomes. These reports benchmark each participant’s data against regional and national outcomes displayed in both graphic and tabular format. Reports are available to participants in electronic web based format.

Launched in 2011, the STS Research Center is a nationally recognized leader in patient outcomes research. With the wealth of data in the STS National Database, the Center supports cutting-edge clinical research that is designed to improve surgical outcomes and the quality of patient care.

Because the STS National Database and TVT Registry do not collect long-term clinical data, linking these registries with the DMF allows for the verification of life status of patients who otherwise would be lost for follow up after treatment.
Utilizing clinical data, combined with claims information and the DMF, STS has been able to provide long-term information on patient treatment outcomes and estimate patient survival rates. STS members use this information to evaluate their respective outcomes against national standards or benchmarks. Outcomes data also help physicians, patients, and their families make informed treatment decisions. The Society also uses this information to facilitate research comparing the long-term effectiveness of alternative treatment strategies based on patient demographics. For example, the American College of Cardiology Foundation-The Society of Thoracic Surgeons Collaboration on the Comparative Effectiveness of Revascularization Strategies ASCERT™ Trial was designed to compare catheter-based and surgery-based procedures using existing databases from the ACC and STS combined patient outcomes data. This research required access to the Centers for Medicare and Medicaid Services’ 100% denominator file data, to examine long-term outcomes following revascularization. ASCERT is just one example of how patients could benefit from the research that could be conducted with continuous access to patient outcomes information like the data contained in the DMF.

If you have a legitimate business purpose pursuant to a law, governmental rule, regulation, or fiduciary duty, explain in detail the basis of that legitimate business purpose and cite the relevant law.

The Society of Thoracic Surgeons has a legitimate business purpose pursuant to the Illinois General Not for Profit Corporation Act of 1986 (“Illinois Act”) and Section 501(c)(6) of the Internal Revenue Code. The quality improvement activities described above illustrate STS’ business purpose and reflect our central mission: “to enhance the ability of cardiothoracic surgeons to provide the highest quality patient care through education, research, and advocacy.”

In addition, the Society is pursuing recognition of the Adult Cardiac Surgery Database as a Qualified Clinical Data Registry (QCDR) under newly implemented provisions of The American Taxpayer Relief Act of 2012. This statute recognizes registries as conduits to fulfill physicians’ quality reporting requirements under the Medicare program. Congress is also currently considering legislation that will allow QCDRs to access Medicare claims data to facilitate quality improvement. This program further emphasizes the importance of the quality improvement efforts in the health care sector – efforts that depend on the ability to assess long term patient outcomes through access to death data.

Do you have systems, facilities, and procedures in place to safeguard DMF information, and experience in maintaining the confidentiality, security, and appropriate use of such information? If so, explain in detail.

As a medical society, STS has long advocated for the protection of patients’ and our members’ privacy. The STS National Database upholds rigorous privacy protocols and is fully compliant with the Health Insurance Portability and Accountability Act (HIPAA), Federal Common Rule protections for human subjects’ research, the Federal Information Security Management Act (FISMA), and other privacy and security regulations. Pursuant to HIPAA, STS has a Business Associate Contract or Data Use Agreement with all STS members, or “covered entities,” who contribute to the STS National Database. In addition, STS and DCRI have a sub-business associate / data use agreement in place because, as The STS National Database data warehouse, DCRI has access to personal health information. This sub-business associate / data use agreement requires DCRI to comply with HIPAA
regulations and those promulgated under the Health Information Technology for Economic and Clinical Health Act.

Further, STS, through its contract with DCRI, maintains patient identifier information separately from the clinical and other demographic data. Externally-derived data, like those from the DMF, are used to supplement the data in the individual record, but these clinical, patient-level data never leave the database except in de-identified form.

The data warehouse at the DCRI maintains STS data in manner compliant with the FISMA (Moderate) analytic system. All DCRI employees sign a confidentiality agreement. This agreement includes clauses that obligate the signatory to ensure appropriate use of confidential data.

If you have systems, facilities, and procedures in place to safeguard DMF information, or to safeguard sensitive information other than DMF information, explain whether and how your systems, facilities, and procedures are audited, inspected or monitored.

Electronic access to stored data is monitored continuously and access logs are reviewed by security personnel. Access to the computer area where the data are stored is restricted and monitored via security cameras. DCRI security procedures are audited annually by the Duke internal audit information technology team.

Auditing, inspection, and monitoring of who accesses protected data are required by HIPAA Privacy and Security regulations (45 CFR 160-164). Routine monitoring is an additional requirement for maintaining FISMA compliance. To the extent that the DMF information would be used for FDA regulated studies, DCRI also complies with 21 CFR 11 which defines the criteria under which electronic records and electronic signatures are considered to be trustworthy, reliable and equivalent to paper records.

If you have systems, facilities, and procedures in place to safeguard DMF information, or to safeguard sensitive information other than DMF information, and if your systems, facilities, and procedures are audited, inspected or monitored, explain whether that is voluntary, or whether it is required by law, governmental rule, regulation, fiduciary duty, or other reason and cite such.

Both the HIPAA and FISMA require that STS and DCRI monitor how sensitive information is used and whether or not that information is shared with a third party. HIPAA requires that we maintain Business Associate Agreements or Data Use Agreements with any third parties that have access to the personal health information we house. These agreements govern how and why this information is shared with third parties.

---

1 Sample confidentiality agreement is available at: [https://www.hr.duke.edu/forms/confidentiality.php](https://www.hr.duke.edu/forms/confidentiality.php)
disclosed and require that any disclosures that are made outside the scope of our agreement be assessed for security or privacy breaches.

If you have systems, facilities, and procedures in place to safeguard DMF information, and experience in maintaining the confidentiality, security, and appropriate use of such information, explain in detail the extent to which these satisfy the requirements of section 6103(p)(4) of the IRC, or satisfy requirements "similar" to the requirements of section 6103(p)(4) of the IRC.

The FISMA requirements are "similar" to section 6103(p)(4) in that both are based on the National Technical Information Service (NIST) 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations."

If you do not currently have systems, facilities, and procedures in place to safeguard DMF information, explain how you would anticipate putting such systems, facilities, and procedures in place in order to become certified to access DMF information.

Our systems are currently sufficient to safeguard DMF information.

Under the Act, you are required to certify that you have systems, facilities, and procedures in place to safeguard DMF information, and experience in maintaining the confidentiality, security, and appropriate use of such information, pursuant to requirements “similar” to the requirements of section 6103(p)(4) of the IRC. Please explain in detail how your systems, etc., and experience might be “similar” but not identical to the requirements of section 6103(p)(4) of the IRC, and how any differences from the requirements of section 6103(p)(4) of the IRC would nevertheless permit achieving the objective of safeguarding DMF information.

As both the Internal Revenue Code (IRC) rule and FISMA are based on the same security standards (NIST 800-53), they should provide similar protections.

What systems, facilities, and procedures do you believe are necessary to safeguard DMF information provided under the Act, including audit, inspection and monitoring procedures?

We believe that complying with the HIPAA security standards (45 CFR 160) or FISMA (Low) standards are more than adequate to safeguard DMF data. As reported above, DCRI is currently FISMA (Moderate) compliant.

Would the imposition of a single, presumably larger, fee at the time of certification be preferable to the charge of multiple, presumably smaller, fees, such as annual fees?

An annual fee would be preferable.
March 18, 2014
The Society of Thoracic Surgeons

In order to become certified to have access to DMF information, how would you prevent disclosure of such information to any person other than a person who was also certified, or who, if not certified, would meet the requirements of certification?

As described above, DCRI maintains Business Associate and Data Use Agreements that meet HIPAA requirements with any third party (person or entity) that has a need to access personal health information. These contracts can be modified to include DMF data.

If you currently access DMF information, does your use of that information include or require the name, social security account number, date of birth, and date of death of deceased individuals? If not, explain which type(s) of DMF information you do not use.

The DCRI received the DMF through Calendar Year 2011. At that time, we used all of the information to match individuals in the DMF to our other databases to ensure we were applying the date of death to the correct individual.

Would you find it useful to access DMF information that included information for a deceased individual during the 3-calendar-year period beginning on the date of the individual’s death, but did not include one or more of the name, social security account number, date of birth, and date of death of the deceased individual? If so, explain which type(s) of DMF information could be excluded.

A 3-calendar-year wait would make the information significantly less valuable to our reporting needs. Because the DMF dropped the state field in 2011, we need all the other fields to feel comfortable with a match.

On behalf of the Society, thank you for the opportunity to provide information on the essential patient outcomes studies and quality improvement efforts facilitated by the STS National Database and DMF data. Based on our stated business purpose and data protection procedures, we feel that our clinical registry should qualify to participate in the DMF certification program. We hope that this certification program will allow clinical registries to continue to access DMF data for quality improvement and research purposes and activities, which are already conducted pursuant to HIPAA regulations, the Common Rule, and other privacy and security regulations. We look forward to continuing to work with you on this effort. Please contact Courtney Yohe, Assistant Director of Government Relations at 202-787-1222 or cyohe@sts.org with any questions.

Sincerely,

David A. Fullerton, MD
President