A climate change rally with over 40,000 participants took place in Washington, D.C., on February 17th. The rally, called Forward on Climate by the organizers, the environmental groups Sierra Club and 350.org, called for government measures to stop climate change, including blocking of the Keystone XL pipeline construction.

Dr. David Hosack (1769-1835) was a "mover and shaker" on New York's medical scene during the early 19th century. While some considered him to be the outstanding practitioner of his era, others reviled him as a liar and trouble-maker. Considered one of the star teachers of the early College of Physicians and Surgeons, he later fomented a faculty revolt that led to a mass resignation from the College, almost destroying it. Hosack then formed his own medical school in lower Manhattan that was affiliated with Rutgers College.

A study called “Assessing the Global Burden of Ischemic Heart Disease” was published in two parts in volume 7, December 2012 issue of Global Heart. http://dx.doi.org/10.1016/j.gheart.2012.10.004

"Ischemic heart disease (IHD) is the leading cause of death worldwide. The GBD (Global Burden of Disease, Injuries, and Risk Factors) study (GBD 2010 Study) conducted a systematic review of IHD epidemiology literature from 1980 to 2008 to inform estimates of the burden on IHD in 21 world regions in 1990 and 2010." (From the abstract)

The first part of the study, which included a systematic review, was conducted by Andrew E. Moran, MD a faculty member at Columbia University Medical Center with help from two librarians from the Health Sciences Library, Marina Chilov and John T. Oliver (now at the College of New Jersey.) The study “highlighted the lack of information about IHD in Sub-Saharan Africa and other low-income regions. More complete knowledge of the global burden of IHD will require improved IHD surveillance programs in all world regions.”

The Health Sciences Library is pleased to present Dr. Michael Nevins speaking on "Dr. David Hosack: ‘Stormy Petrel’ of American Medical Education" on Wednesday, March 13 at 6:00 PM (refreshments will be served at 5:30 PM) in Russ Berrie Medical Science Pavilion, Room 2, 1150 St. Nicholas Avenue at West 168th Street.

Dr. David Hosack (1769-1835) was a "mover and shaker" on New York’s medical scene during the early 19th century. While some considered him to be the outstanding practitioner of his era, others reviled him as a liar and trouble-maker. Considered one of the star teachers of the early College of Physicians and Surgeons, he later fomented a faculty revolt that led to a mass resignation from the College, almost destroying it. Hosack then formed his own medical school in lower Manhattan that was affiliated with Rutgers College.

The Health Sciences Library is pleased to present Dr. Michael Nevins speaking on “Dr. David Hosack: ‘Stormy Petrel’ of American Medical Education” on Wednesday, March 13 at 6:00 PM (refreshments will be served at 5:30 PM) in Russ Berrie Medical Science Pavilion, Room 2, 1150 St. Nicholas Avenue at West 168th Street.

Dr. David Hosack (1769-1835) was a “mover and shaker” on New York’s medical scene during the early 19th century. While some considered him to be the outstanding practitioner of his era, others reviled him as a liar and trouble-maker. Considered one of the star teachers of the early College of Physicians and Surgeons, he later fomented a faculty revolt that led to a mass resignation from the College, almost destroying it. Hosack then formed his own medical school in lower Manhattan that was affiliated with Rutgers College.
Prepping Your Computer for Encryption

The Endpoint Security Campaign that was launched in December is requiring full disk encryption with pre-boot authentication on any computers containing Patient Health Information (PHI) and Personally Identifiable Information (PII). CUMC IT is also recommending that everyone use encryption on their computers in order to protect other sensitive data and help insure that lost or stolen equipment does not lead to a security breach, which can have costly penalties for both the individual who uses the computer and the institution – even if the equipment is personally owned.

By nature, encryption software makes data unreadable without proper verification. When it is first set up there is always a small risk that data will be lost or that other issues may arise. Be sure to take these important steps when preparing a computer for encryption.

Do a full backup of your data before encrypting – if the backup contains sensitive information the backup media must also be secure and encrypted, and cannot be stored with an external vendor like iCloud or Dropbox that do not have a signed agreement with CUMC to adequately protect this data.

- Windows and Macintosh OS X have built in back up programs that can automate this for you. On Windows go to Backup and Restore in the Control Panel. On Macintosh select Time Machine from your System Preferences.
- Full backups will usually require a large external drive, but if you just want to back up specific folders and files you can manually copy them to an encrypted USB key or discs.

Make sure you have copies of software installation files, licenses and any keys that may be needed in case programs need to be reinstalled. This includes your operating system and any drivers that the computer uses.

- If your computer came with system discs when you purchased it, keep these as they will contain the software needed to repair or reinstall the OS and drivers. Using them will be much quicker than hunting for individual drivers online for your computer’s specific hardware configuration.
- If no discs were included be sure to create recovery or repair discs yourself as soon as possible. These will come in very handy if the computer crashes at any point.

Verify that your computer is compatible with encryption software requirements.

- Macintosh systems must be on Snow Leopard (10.7) or Mountain Lion (10.8) to run the approved version of OS X’s encryption, FileVault 2. If you are using an earlier version you will need to upgrade.
- Windows computers may need to be running an edition higher than the Starter or Home versions that are usually installed on store bought systems. Look in the System information in the Control Panel for your Windows edition.

Pick a strong encryption password that you will not forget.

- Encryption by nature will scramble data so it cannot be viewed without proper authentication, and may even completely destroy it after a few bad login attempts.
- Do not use this password for anything else. If another system is hacked and has your password information it could easily be tried to decrypt sensitive data.

Use any encryption master or recovery key options. Most programs provide an alternate way to decrypt data if the original password is forgotten. When creating one be sure to store it in a secure place.