As *The New York Times* has noted, “Bill Hayes has an unusual set of skills: part science writer, part memoirist, part culture explainer.” For his three nonfiction books to date, he has gone to unusual lengths in pursuit of his subjects. Hayes spent a year studying anatomy alongside medical students for his acclaimed book *The Anatomist: A True Story of Gray’s Anatomy* . He is now at work on a history of exercise, titled *Sweat*, for which he is delving into the life of sixteenth-century physician and early exercise advocate Girolamo Mercuriale. Hayes will retrace his steps in researching his books and discuss the varying approaches he has taken in writing about the human body.

Please join us on Wednesday, March 4th, in Room 1 of the Russ Berrie Pavilion at 5:30pm for refreshments, followed by the lecture at 6pm. The Russ Berrie Pavilion, at St. Nicholas Ave. and West 168th Street, is easily reached by the A, C, and 1 subway lines and numerous bus routes.

**Digital Collections - History of CUMC**

Since 2010 the Health Sciences Library has been a member of the Medical Heritage Library, a consortium of some of the country’s leading biomedical libraries. The MHL is devoted to “free and open access to quality historical resources in medicine.” With funding from the Sloan Foundation, the Metropolitan New York Library Council (METRO), and the National Endowment for the Humanities, the Health Sciences Library has been able to digitize over 6000 volumes (over 2 million pages) relating to the history of the biomedical sciences, broadly interpreted. Of these, several hundred relate to the history of the Columbia University Medical Center including its four health science schools and affiliated hospitals.

Access to the over 60,000 items in the Medical Heritage Library, including rare books, pamphlets, journals, and films, can be found in the Internet Archive.

Learn more at: [http://tiny.cc/1pxrux](http://tiny.cc/1pxrux).
FCC Votes in Favor of Net Neutrality

On February 26th, 2015 the Federal Communications Commission voted to reclassify broadband providers as a telecommunications service. This brings companies supplying high-speed Internet under regulations that are similar to public utilities, and to those regulations by which mobile voice networks have been governed for the past twenty years.¹

This is seen as a huge win for net neutrality supporters, who demanded that network providers should not have the ability to change the speed of or completely block access to legal forms of online content. The vote came on the heels of a court decision last year that the FCC could not enforce regulations against broadband providers as they were then classified, and a public statement released by President Obama in support of reclassification.

The FCC rules will not include rate regulation, but do ban blocking, throttling and paid prioritization. Without oversight there was great concern that companies like Comcast, Time Warner and Verizon could bill content providers for increased speed of delivery, effectively pricing out start-ups or smaller companies. Those opposing regulation believe this would provide broadband companies with funds they could then use to upgrade and expand broadband infrastructure or foster their own innovative content and applications.

The full rules are still to be published, and lawsuits challenging the change are widely expected.


Phishing Season

Tax season can bring an onslaught of phishing messages from attackers imitating the IRS or other government and finance-related entities. Make sure you know how to spot and report phishing attempts.

- Phishing related emails, texts, and even phone calls often stress urgent action or response to try to prevent anyone from double-checking an issue. Information in the message also tends to be vague, such as “update your account”, though more sophisticated attempts may use details that seem specific but can be found on the official entity’s website or other open publication.

- Never click on a link or reply to a message that seems suspicious. In some cases hovering your cursor over a link will reveal a spoofed address and immediately give away the attempt. Go directly to a known address for the sending entity such as www.irs.gov by manually opening your web browser and typing it in, then use links on the main website to look for pertinent information. If still unsure contact the sender directly by a valid phone number or email address.

- To report suspicious messages received in your CUMC or Columbia email account see this FAQ: http://www.cumc.columbia.edu/it/howto/email/faq.html#spam

- If you end up giving out information without realizing it was a phishing attempt, change any online password and contact appropriate support immediately. Your CUMC email password can be changed instantly via the myPassword link on the CUMC IT home page: www.cumc.columbia.edu/it