Research finds open-source software is actually more secure for health care IT

March 8 2011

Globally the sale of health care information systems is a multibillion dollar industry. The vast costs, frequent failed systems, and inability of systems to talk to each other regularly attract media comment. However policy makers still shy away from a class of software, Open Source, that could address many of these problems, because of worries about the safety and security of Open Source systems. Now new research by the University of Warwick's Institute for Digital Healthcare, and the Centre for Health Informatics and Multiprofessional Education at UCL Medical School, finds that Open Source software may actually be more secure than its often more expensive alternatives.

Dr Carl Reynolds of UCL's Centre for Health Informatics and Multiprofessional Education said:

"Software bought or otherwise distributed under a licence which require it to come bundled with the source code and the right to freely edit, reuse, and share it is called free or open source software. Such a licensing arrangement leaves the buyer in a very strong position when compared with the usual proprietary licences. The buyer is less prone to lock-in, where a buyer loses the ability to switch software products because of the use of proprietary data formats or restrictive licensing conditions. When the buyer chooses an open or free licence he or she can take the code to a rival code developer if they offer a better deal. If the code is in the public domain, and the user and programmer community are engaged, then the buyer can profit from more people inspecting and fixing the code leading to higher quality source code and

in turn software."

Professor Jeremy Wyatt of the University of Warwick's Institute for Digital Healthcare said:

"Critics of Open Source often argue that, because the code is public, an attacker can more easily find and exploit vulnerabilities. But our work at the University of Warwick and UCL shows that the evidence does not bear this out and in fact Open Source Software (OSS) may be more secure than other systems.

"Proprietary systems often rely on a 'security through obscurity' argument, ie that systems that hide their inner workings from potential attackers are more secure. However security through obscurity alone completely fails when code is disclosed or otherwise discovered using tools such as debuggers or dissemblers. Worse, it has been suggested that the cloak of obscurity tends to encourage poor-quality code. Opening the source allows independent assessment of the security of a system, makes bug patching easier and more likely, and forces developers to spend more effort on the quality of their code."

The researchers also refute the argument that using Open Source Software (OSS) is inherently riskier because one automatically becomes liable for any failings of the software. They say that "typically a large organization will pay a contractor for an OSS implementation and support package. Many contractors providing OSS implementation and support offer legal indemnity to clients in exactly the same way as proprietary vendors."

More information: The researchers' paper entitled "Open Source, Open Standards, and Health Care Information Systems" by: Dr Carl J Reynolds, Centre for Health Informatics and Multiprofessional Education, UCL Medical School and Professor Jeremy Wyatt of the

University of Warwick's Institute for Digital Healthcare, has just been published in the *Journal of Medical Internet Research* at www.jmir.org/2011/1/e24/