Wireless drug control

February 6 2009

Electronic implants that dispense medicines automatically or via a wireless medical network are on the horizon. Australian and US researchers warn of the security risks in a forthcoming issue of the *International Journal of Biomedical Engineering and Technology*.

With the advent of personalized medicine, advances in diagnostics and the miniaturization of sensors and control systems for delivering drugs automatically, the Remote Intelligent Drug Delivery System (RIDDS) may soon be a reality. Such devices, implanted under the skin, would remove the inconvenience of manual drug delivery. By connecting a RIDDS to a wireless medical control centre wirelessly patients with physical disabilities, learning difficulties, or who are otherwise unable to give themselves medication could benefit.

RIDDS device will have inbuilt sensors to monitor biomarkers of a patient's symptoms, pulse rate, or blood oxygen levels, for instance. Wireless control will allow healthcare workers to monitor the patient's health as well as device behavior. They could adjust medication frequency or levels as necessary based either on direct patient observation or sensor outputs. However, one aspect of RIDDS deployment that is yet to be addressed is security.

YanYan Wang and Carey Thaldorf at the University of Central Florida, in Orlando, USA, and colleague John Haynes of Charles Darwin University, Darwin, Australia, outline the security risks of RIDDS in a forthcoming issue of IJBET, and present some possible countermeasures.

They point out that any wireless communications technology is open to various security issues, which may fall under the generic umbrella of hacking, or cracking, including eavesdropping, jamming, and tampering. A hacker could intercept and alter transmitted data, they might steal personal information, or someone with malicious intent might spoof the sensor outputs of a RIDDS. It is not beyond the bounds of possibility to imagine that such a person, having hijacked the RIDDS connection might trigger commands to release medication inappropriately and so harm or even kill a patient.

"We have raised security concerns in relation to RIDDS, especially in the context of medical sensor networks, because, among other reasons, a failure to do so could risk the privacy and possibly the life of a patient," the researchers say. "The dilemma in RIDDS makes adoption of the technologies intimidating," they add. The team concludes that, "Security mechanisms for RIDDS must be fully considered prior to the widespread deployment of such delivery systems."

More information: *Int. J. Biomedical Engineering and Technology*, 2009, 2, 135-151 "Security risks for remote intelligent Pharmacy-on-a-Chip delivery systems" by YanYan Wang, John Haynes, and Carey Thaldorf

Source: Inderscience Publishers

Citation: Wireless drug control (2009, February 6) retrieved 18 April 2024 from https://phys.org/news/2009-02-wireless-drug.html