Securing eprescribing with strong authentication

Barry Chaiken, Imprivata

To achieve higher levels of quality, patient safety, and efficiency in healthcare delivery, the National Health Service has invested large sums of money in a variety of health information technology tools over the past decade.

Although accrued benefits from utilising these new tools are arriving more slowly than expected, both researchers and clinicians who are deploying these tools are confident they will provide the expected value.

This confidence draws from the expanding number of success stories reported both in the UK and in the US, where the American government has invested heavily in implementing electronic medical records in both hospitals and physician offices.

Electronic prescribing (eprescribing) — digitally-based recording and transmission of medication orders — is one of the technology advancements that offer physicians advantages in efficiency and patient safety.

These benefits drive high levels of adoption and satisfaction among physicians using this health information technology tool. Recognising the responsibility of protecting patient data, NHS trusts utilising eprescribing must facilitate e re-authentication for physicians, without changing their workflow.

Introducing new and cumbersome workflows with overly complex and disruptive sign-on and authentication processes can of the eprescribing system by physicians, or to an unsecure patient data repository that facilitates prescription writing erro

Failure to strongly authenticate users each time a prescription is written presents significant problems for patients, clinician implemented eprescribing systems may lead to the ordering of inappropriate medications by clinicians on patients not their

In a busy healthcare setting where multiple clinicians share a computer terminal, failure to authenticate can easily confuse patient being treated and the illness under consideration. Errors can occur unnoticed, leading to poor clinical outcomes and unnecessarily treating drug reactions due to medication errors, or worse scenarios.

With this in mind, in order to optimise the benefits of eprescribing while maintaining high levels of security, trusts need to non-repudiation of eprescriptions. To specifically tackle the security challenges associated with eprescriptions, trusts can in of authentication at the transaction level.

By demanding that users re-authenticate at the point of issuing a prescription, healthcare organisations can benefit from n records, offering an assured link from a prescription back to the clinician who placed the order.

Multiple combinations of strong authentication exist, usually including two of three factors:

1. something you are, eg fingerprint biometric;
2. something you have, eg smart card; or
3. something you know, eg password.

Such authentication offers a secure, reliable, and easily utilised method of accessing sensitive personal health information data from unauthorised users. Recently, the Information Commissioners Office (ICO) heavily criticised the NHS for the larg security breaches and data losses among the Trusts.

With penalties of up to £500,000 for such instances, trusts must seriously consider deploying strong authentication technol patient health information while facilitating clinician workflow.

Effective utilization of health information technology demands an efficient and secure user log-on and authentication proce of use to clinicians. The technology must fit the requirements of human users rather than having the humans adapt to the

It is also clearly easier to modify and replicate technology to meet the needs of clinicians than to continually retrain clinicia introduction of new technology.

Barry P Chaiken MD MPH, CMO, Imprivata.