In the battle to keep confidential data safe, patients shouldn’t be on the losing side

Healthcare providers certainly have a challenge in keeping patients’ data confidential. Information Governance has a huge role to play, with any devices used having to meet stringent guidelines.

Vulnerability of data
Information Governance guidelines rule on the ways that patient data is captured, stored, maintained and shared. Unfortunately for patients, a glance at mainstream news in the last 12 months shows plenty of stories of how their confidential information was left exposed by healthcare providers or the victim of some form of cyber-attack. There are certainly processes in place to ensure that data is kept safe but adhering to these protocols isn’t always so simple. Vulnerability certainly appears where there is a difference in how each department manages and safeguards data – or the variety of devices that are used to collect and store patient data.

The challenges faced
With an increasing indifference to how best practice is actually implemented, many opportunities for data breaches have the potential to occur and be reported in the press. Simply type ‘hospital data breach’ in any search engine and recent news stories of where data has fallen foul to some form of negligence will come out. This leads to a lack of public confidence that healthcare providers are able to keep personal data stored securely and, most importantly, only shared with relevant parties.

The importance of security
Maintaining and safeguarding up-to-date patient data is crucial. Not only for keeping data private but also when needed for further medical appointments or emergencies. With so many different medical professionals who may need access to personal information at any time, there’s no doubt that keeping this data safely available is so important. Regardless of the equipment used to register, update or access patient data – whether it’s a PC, tablet, voice recorder, etc – best practice recommends that analogue tapes are no longer sufficient to meet regulations, and despite guidelines many healthcare entities still record patient data through unsuitable and unsafe devices.
Helping IT deliver better solutions
A great concern with analogue tape devices is the threat that anyone can access particularly sensitive data. And with hospitals in particular, keeping control of where each device is, or who has access to it, can also pose a risk. Which is why it’s essential to adopt digital devices that can be kept under central management for ease of identification, with secure control of use. Philips digital voice recorders allow IT staff to manage users, licenses, and system settings remotely. Hardware administration can also be done centrally for convenience of device configuration and firmware updates.

Highly secure digital voice recorders
The Philips PocketMemo 8000 series offer various layers of security that can be configured to suit individual needs. A user will only have a certain number of times to enter a password to activate the voice recorder. Patient data can be scanned through an integrated barcode and linked to a recording. This ensures reliable assignment of patient IDs and speeds up data digitalization workflow. The data is encrypted in real time using the Advanced Encryption Standard (AES) with a key length of 256 bits, therefore inaccessible to unauthorized persons. If a recording device is linked to a PC, it opens up possibilities of data being misused - this is where the PocketMemo 8000 enables central management by IT. The technology allows identification of device, user, and serial number automatically; preventing the recorder from being used where it shouldn’t. The device’s unique Mass Storage Protection feature prevents other data being put on the recorder and moved off site or outside of the dictation workflow. The devices can be administered remotely, so users, licenses, system settings and firmware can be centrally managed.

HOW PHILIPS CAN HELP
Finding the right voice technology
For healthcare providers in search of a solution to securely record and manage sensitive data, the challenge is on to discovering products that are simple to use and benefit from the most up-to-date technology. Philips SpeechExec Pro is a sophisticated speech-to-text workflow software that links dictation authors and transcriptionists. This means that medical staff can securely record their notes through digital voice recorders such as Philips SpeechMike, SpeechAir, or the PocketMemo, and send the sound files to secretaries, ready for transcription. The result is not only faster turnaround times for written documents, but the whole process is safe from a data security standpoint. Additionally, Philips hardware and software easily integrate with medical systems.

A step further with speech recognition
Voice recognition technology can be used to create the same notes, documents, emails and reports that are currently being created by typing. Repetitive tasks can be completely automated so healthcare staff can use their expertise in a far more productive way. Philips SpeechExec Pro 10 software comes with integrated voice recognition technology tailored to vocabulary used in the medical sector. Furthermore, the software ‘learns’ as it is used, increasing speech recognition accuracy up to 99%.

About Philips Speech Processing Solutions
Philips Speech Processing is the global driving force in voice technology innovations for over 60 years. Always putting emphasis on outstanding quality, the company has designed ground-breaking products, such as the digital voice recorders SpeechAir and PocketMemo. The SpeechMike is the industry leading dictation microphone, now in a cordless version with the release of SpeechMike Premium Air. The company’s latest software innovation, SpeechExec Pro 10, combines professional voice recognition and voice-to-text workflow management for businesses. The Philips voice recorder app for smartphones coupled with Philips SpeechLive take dictation and transcription securely to the cloud, making workflow processes faster than ever before.