Two of the big players have recently entered the personal health records (PHR) market. In October 2007, Microsoft\textsuperscript{1–3} launched ‘HealthVault’ \<www.healthvault.com/>. This free portal allows individuals to manage their health records. It comprises three sections: HealthVault Search – for searching for health information on the web; HealthVault Account – ‘to collect, store, and share your health information with websites and doctors’; HealthVault Connection Center – to ‘Connect a wide variety of HealthVault-compatible devices from partners to your PC, and upload the data to your HealthVault account’. Apart from the search facility, HealthVault is currently only available in the US. In the same month, Google\textsuperscript{4,5} announced that it was also planning to offer a facility for online PHRs. The NHS has been offering HealthSpace \<www.healthspace.nhs.uk/> for some time. This is ‘a secure, online, personal, health organiser’. Access is initially via a registration process that requires some personal details and an email address, and after that via id/password. Once again in October 2007, the NHS\textsuperscript{6} announced the pilot of a system whereby individuals can view their summary care records on HealthSpace. This pilot is only available to people in an Early Adopter area for the NHS Care Records Service. People wishing to access their summary care record will have to undergo a further registration process that validates their identity, and generates a smart card for on-going access.

EMIS, a major IT supplier for primary healthcare in the UK, is also piloting\textsuperscript{7,8} people’s access to their records with a number of GP
He@lth Information on the Internet

surgeries. Their plan is to roll this out across all their practices. PHRs are in their simplest concept a way of providing an individual with access to details of their healthcare. As such, they can be either paper or electronic. But, with the development of interactive Internet-based tools, electronic methods have moved on from portable devices such as CDs, to a networked record that can be shared between the individual and healthcare providers and exchange data with the provider’s electronic records management system (ERMS). Pagliari et al. provide a good discussion of the topic. They conclude: ‘that, amongst other benefits, ePHRs have the potential to improve communication between providers and patients by sharing information, to enhance the quality of care and involvement in their own health and illness’. The driver in the UK, with a national health service, appears to be one of patient empowerment and involvement in their own care. The driver in the US, with a private, distributed healthcare market, appears to be the realisation that the only person with the motivation to establish a cradle-to-grave health record is the individual themselves.

The American Health Information Management Association (AHIMA) has set up myPHR (www.myphr.com/index.asp) – ‘A guide to understanding and managing your personal health information’. As well as advising on how to set up a PHR, it also provides a searchable database of PHR tools.

I can see three main problems with PHRs. First, there are no standards so incompatibility between different systems is a problem, particularly with the integration of PHRs with ERMS. Second, in a non-NHS set up, there are no guarantees that an organisation providing a PHR system will continue, so at worst individuals can risk losing their data, at best they will have to continually migrate their data between systems and organisations. Third, and most seriously, is the problem of security. As IT people know, any data on a network is vulnerable and encryption can be broken. However, the weakest link is the people aspect – not the end user, but the organisations themselves. They have a terrible record of protecting confidential data as the following examples show: financial details in paper format dumped, unshredded, by banks in their dustbins; laptops containing confidential data stolen or left in taxis; government departments sending personal data on CDs by postal service, unencrypted and only protected with a password; a web hosting company, successfully hacked, who had stored their customers’ passwords in unencrypted text. The NHS is not immune. Recently, Connecting for Health announced a ‘clampdown on deliveries of unencrypted data sent by regular mail services’ to the NHS Strategic Tracing Service. Until organisations take security of personal data seriously, perhaps PHRs are a step too far.

References/Resources
1. <www.pcmag.com/article2/0,1759,2191920,00.asp>
2. <www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9041142>