Hypocritic Oaths

Medical records have lost their way.

By Duncan Campbell

***Guardian*, 5 November, 1997**

Britain's medical computer networks are a "recipe for disaster" for security and privacy, it was claimed this week. They have already cost patients' lives and wasted hundreds of millions of pounds, said Ross Anderson, the Cambridge specialist who is also the British Medical Association's adviser on information security. Speaking in Brighton on Tuesday at Medtel, the World Congress on the Internet in Medicine, Anderson warned that "more and more public health information is being sucked from clinical systems towards the centre. The effect is that we have a terrible aggregation of sensitive data to which more and more staff have access."

GPs and health care providers were increasingly being compelled to provide far more personal data on patients than was needed to meet accounting or management criteria, leading to the wide distribution and availability of highly confidential medical data.

In particular, there was "consternation, horror and outrage" earlier this year when charities providing support services to people with HIV and Aids learned that information they had supplied to health authorities was being used to identify their clients. Department of Health staff had lied, said Anderson, when they reassured clinicians that personal health data being fed into the NHS network was not even linkable, let alone identifiable.

Anderson said there were many areas where privacy was being undermined. He highlighted a new NHS administrative register that will record every association that a patient makes with a healthcare provider, including special GUM (genito-urinary

medicine) clinics. If the register showed that someone was getting treatment from a remote GUM centre, this would be a “dead giveaway”, he noted.

Other areas included the national clearing system to pay fundholding GPs’ bills, in which confidential data was being harvested through health authorities and shared around the country, without controls for relevance or timeliness. Personal privacy was also being cracked in Whitehall in a “Hospital Episodes System” database, which contained information about hospital visits that are supposedly anonymous. The data will identify more than 98 per cent of the population, and also track patients. The result is “a shadow medical record kept at the health authority outside clinical control”.

Another area, said Anderson, is the data gathered by the Newcastle-based Prescriptions Pricing Authority (PPA), which is used to pay pharmacists; this information is available to Whitehall departments, including the Home Office. The Government had failed to reply to enquiries by the BMA as to whether the data was being exploited to detect and track illegal immigrants or others of official interest.

These claims come just as the NHS Executive has launched NHSnet, a national communications systems for doctors, hospitals and health managers run by BT and Mercury. Anderson’s campaign of trenchant criticisms of NHS computer security and privacy has already led to a wide-ranging and heated debate about whether Britain’s medical network is safe.

The NHS Executive’s information management group acknowledges that Anderson’s campaign has “had some useful results. [He] forced the pace in the Department’s careful consideration of measures for NHS-wide encryption.” But the group claimed that “it is a matter for regret that the campaign has generated a substantial number of misunderstandings”.

Undeterred, Anderson repeated his warning this week that “a serious and large scale violation of privacy” was taking place. According to the North Yorkshire Health Authority, staff specially trained to vet medical inquiries found that there were 30 illegal attempts every week to obtain unauthorised access to personal information. Nationwide, this could mean more than 250,000 unauthorised attempts a year to gain personal medical information.

“The main privacy risks come from aggregating data,” said Anderson. “It’s not about external hacking; it’s about use of information by inside abusers. The most vulnerable people come off worst.”