IN 2000, a computer error at a Sheffield Hospital in Britain led to pregnant women being put in the wrong risk category for Down syndrome babies. The system misdiagnosed the ages of the expectant mothers, 158 of whom were told they were at low risk when in fact they were in a high-risk group.

Had they known the truth they probably would have proceeded with further screening that would have revealed six had pregnancies affected by Down syndrome. It was later revealed the computer software was not Y2K compliant.

It's the kind of horror story that can erode public confidence in the systems set up to create greater efficiency and accuracy. And that, said Queensland University of Technology's Peter Croll, was critical.

Professor Croll, director of QUT's Centre for IT Innovation, is investigating the risk exposure in electronic health systems.

"What we are doing is making sure that the system does not fail and that trust is not eroded, and that IT brings the benefits that people believe it will," he said. "The danger is believing that IT will improve things regardless."

While acknowledging the benefits of e-health systems, Professor Croll said they could also endanger people's lives.

Abuse of computer records, missing data or the input of wrong information can have catastrophic results.

Professor Croll's research began about two years ago when he was at Wollongong University.

He has been working on a model for assessing risk exposure in e-health systems.

The model, called Q.U.i.P.S (derived from the Latin, quippe, meaning to be sure) is being deployed to assess the risk exposure of a community health system used in two regions in NSW and trialled in Queensland.

This health system mostly comprises data on patient appointments and medical records used in community health services such as child care and mental health.

This is being expanded to include in-patient care where live data on patients is recorded on hospital rounds.

Professor Croll cites three things that make a system successful: its usability (degree of use, acceptability of users), safety and privacy (system security and patient confidentiality).

He works closely with the users of the data, such as hospitals, and analyses directly what happens in the field.
That means identifying hazards, developing software to monitor and prevent this, and provide some type of warning system.

This report appears on australianIT.com.au.