



Responding to requests from patients to delete their identifiable data

PIAG has requested UKACR to develop explicit guidance for cancer registries advising them that they must comply with requests from patients to delete identifiable data about themselves from their databases.

Whilst it is possible to delete a patient's record or details from a database, good practice means that information is retained about the process of deletion, to create audit trails in the interests of security. This raises the question as to whether this audit trail should include patient identifiable details to be retained.

Even if complete deletion is effected, this does not guarantee that the same patient will not be added back in, if information is provided from a new source of information. Cancer registries operate on a principle of multiple source ascertainment and information may be provided about the same patient at several points in the care process. The only way of overcoming this would be either to check the database regularly for the presence of a specific patient or to cross check all incoming registrations against a listing of patients who have asked to be deleted. The latter option is in use in some registries as a means of identifying, on receipt of electronic notifications, registry staff members who may have a cancer diagnosis and restricting access to their records by colleagues. Both of these options involve maintaining a database of some means of identification for all patients in this category.

Not knowing about a single case may have important public health effects. A published example [*Epidemiology Community Health* (1994), 48: 232–236] is the investigation of a potential cluster of leukaemia and non-Hodgkin's lymphoma in 0–14 year old children living in the vicinity of the Dounreay Nuclear Reprocessing Plant between 1968 and 1991. There were 9 cases in this age group. Great care was taken to ascertain and verify all cases. With all 9 cases the increased risk (2.58 times higher than expected) was statistically significant (95% CI 1.18, 4.90). If only one case had not been known to the registry (e.g. after being deleted), the increased risk (2.29 times higher than expected) was NOT statistically significant (95% CI 0.99, 4.13), with potentially different actions resulting.

UKACR policy

This is evidently a complex issue and involves balancing the confidentiality of the patient's information against the loss to the person concerned, relatives and to society incurred of not being able to use that information.

The UKACR had adopted the following policy:

Three options are to be presented to patients who wish to opt out of the cancer registration scheme:

- Option 1: the registry will retain the record but flag it to ensure identifiable data are not released to any research projects involving patient contact
- Option 2: the registry will delete all clinical details currently held but will keep a record of the patient's ID in order to delete any information received at a later date
- Option 3: the registry will delete all records currently held, including the patient's ID - this will mean that any data received in the future will not be able to be linked to the request for deletion and so will be processed in the normal way.

A patient wishing to opt out of the scheme will be required to complete the standard data subject notification form (attached) indicating which of the three options he/she wishes to pursue.

The registry receiving a request from a patient to opt out of the scheme under the above options should:

- Option 1: identify any releases of identifiable data about the patient - this should include releases to other registries, ONS and researchers, where this would involve patient contact; instruct these bodies to flag the record on their live database as not to be used for research for patient contact
- Option 2: identify any releases of identifiable data about the patient - this should include releases to other registries, ONS and researchers; delete all clinical details from their live database and destroy any paper records but retain a record of the patient's ID; instruct any other bodies to whom the data have been released to delete the record from their live database and destroy any paper records. All registries contacted or required to delete data should retain a record of the patient's ID
- Option 3: identify any releases of identifiable data about the patient - this should include releases to other registries, ONS and researchers; delete the record from their live database and destroy any paper records; instruct any other bodies to whom the data have been released to do the same.

Additional note:

If a registry is contacted by a patient who resides outside of that registry's region, but who has received treatment within that region, the contacted registry should take overall responsibility for managing the request. The contacted registry should pass the details on to the registry responsible for the area of residence so that the required action(s) can be taken. When the registry responsible for the area of residence has completed the required action(s) they should inform the contacted registry to enable the contacted registry to sign the declaration to the patient that their chosen option has been implemented.

This policy was accepted as a standard for operation from 1st Jan 2004 and revised 1st March 2007 and 20th June 2007.

Last amended: 7th August 2007