Association of British Insurers

ABI PRINCIPLES FOR REQUESTING AND OBTAINING MEDICAL INFORMATION ELECTRONICALLY FROM GENERAL PRACTITIONERS

BACKGROUND

Why insurers use health and lifestyle information to understand and predict risk

Life insurers, like all insurers, use information to understand about an individual when deciding whether or not to offer them insurance cover and, if so, at what level. As life insurers are providing protection insurance cover to give financial protection at a time of ill health, disability or loss of life, much of the information they need to understand the risks posed is health and lifestyle related.

Generally, there are two types of health information an insurer will use to help understand risk. The first is anonymised aggregated population level data. This does not identify individuals but seeks to understand trends in mortality and morbidity across populations and helps insurers to understand how those trends may continue or change in the future. This enables insurers to make cover available to as many people as is possible, even those who have, or who have previously suffered from, severe medical conditions such as cancer, major organ transplantation and HIV infection. In practice, this ensures that some level of insurance cover can be offered to almost everyone.

The second type of health information relates to the individual that is applying for insurance cover. Initially, the insurer will typically ask the applicant questions about their personal medical history, relevant family medical history and about their lifestyle (e.g. if they are a smoker, how much alcohol they drink etc). In addition, medical evidence in the form of reports from attending doctors and screening examinations and tests might also be requested. However, the majority of insurance policies are accepted upon the basis of the information obtained from the application form, without the need of any additional medical evidence.

These two types of information allow the insurer to assess the risk of an individual and decide what level of insurance cover they may be able to offer at a price which reflects the individual's risk. The insurer will only ask for and use information that is relevant to the risk being insured.

How insurers request consent to obtain health and lifestyle information

When applying for insurance, should an insurer require further information, an individual will typically be asked to complete a declaration that provides their consent for the insurer to obtain relevant medical information from their GP. This is performed in accordance with the Access to Medical Reports Act 1988 (AMRA), which determines how insurers, and other third parties, should request medical information from GPs and must include the explicit consent of the individual. AMRA is applicable to Wales, Scotland and England. In Northern Ireland, a request is made under the Access to Personal Files and Medical Reports (Northern Ireland) Order 1991.These two acts give insurers the correct legal route to obtain medical information.

In the past, a minority of life insurers used Subject Access Requests (SARs) as an alternative to the traditional report requested from GPs. The right for individuals to obtain medical records

through SARs is permitted under the Data Protection Act 1998 and insurers were obtaining this medical information by requesting a declaration of consent from the individual, at the time of application. However, in July 2015, the use of SARs for insurance purposes was reviewed by the Information Commissioner's Office (ICO) who expressed concerns regarding this process and possible Data Protection issues that it could potentially create. As a result of their findings, life insurers previously using SARs have withdrawn requesting them and are only pursuing solutions using the AMRA (or Northern Ireland equivalent) process.

In looking to improve the current system, and whilst continuing to use AMRA, any new electronic solutions being developed (1) must continue to allow GPs and insurers to be compliant with their data protection obligations and (2) should be efficient and reflect modern technological demands and evolving customer expectations.

The case for obtaining medical information electronically

An electronic process for obtaining medical information can offer numerous benefits to GPs, insurers and individuals applying for insurance cover by:

- Offering greater protection and more robust security of individuals' sensitive personal data, whilst reducing the risk of irrelevant data being shared with insurers.
- Speeding up the application process, ensuring valuable insurance cover is put in place more quickly.
- Ensuring insurers receive the relevant medical information that they need to offer cover, which in turn offers individuals greater certainty when claiming as the right information has been given to the insurer.
- Reducing the need for insurers to go back to GPs to ask for further details.
- Reducing the time GPs spend on replying to requests.
- Improving the ability of GPs to consistently meet their data controller obligations.

The need for these Principles

In developing new electronic processes in order to gain medical evidence, insurers understand the imperative for any new process to continue to meet the safeguards of the current system. Insurers also appreciate that in order for these new systems to be used by GPs they will need to have absolute confidence in any new process before deciding to use it. The objective of these principles is to demonstrate that insurers understand the importance of how medical information is treated and that, provided these principles are followed, a GP can be confident the process is as safe as the current system and, in some areas, is even more robust in ensuring GPs are better able to meet their obligations as a data controller under the Data Protection Act 1998.

How these principles have been drafted

These principles have been drafted by the ABI and its members with input from the Information Commissioner's Office and the British Medical Association. The General Medical Council has also confirmed that these principles are consistent with its guidance.

Association of British Insurers

PRINCIPLES FOR OBTAINING MEDICAL INFORMATION ELECTRONICALLY FROM GENERAL PRACTITIONERS

1. **All requests must be made in accordance with an individual's rights under relevant legislation**
   Electronic requests must be processed in accordance with the Access to Medical Reports Act 1988 or the Access to Personal Files and Medical Reports (Northern Ireland) Order 1991, with electronic requests allowing medical practitioners to adhere to the key principles of these pieces of legislation. The key aspects include: enabling the individual to see the report, request amendment or withholding of the report, prior to sending it to the insurer, if requested by the individual; retaining copies of reports provided to the insurers for at least 6 months; and, providing a copy of the report to the individual on request within 6 months.

2. **An electronic process must comply with relevant legislation and be reviewed upon fundamental changes to that legislation**
   These principles should comply with relevant legislation, in particular the key requirements of the Access to Medical Reports Act 1988 - and an individual's rights under that Act - and the Electronic Communications Act 2000. The Principles should be reviewed if there are ever notable problems with such systems and whenever relevant legislation, regulation or regulatory guidance is updated.

3. **An electronic process should provide the GP with the ability to redact, amend or add sensitive personal data to an electronic report**
   Any electronic system should provide the GP with the ability to automatically and manually redact, amend or add sensitive personal data to an electronic medical report before it is sent to an insurer, to protect GPs' and insurers' responsibilities as Data Controllers under the Data Protection Act 1998. A Data Controller is any person (which can mean an individual or an organisation) which determines when and how personal data is processed, and their responsibilities include ensuring that the data is accurate and that it is adequate, relevant and not excessive.

4. **An electronic process should be clear about what the patient is being asked to provide to the insurer**
   The process for requesting customer consent for obtaining medical information must make it clear to the individual exactly what consent they are being asked to provide, and do so in a clear, straightforward manner.

5. **An electronic process must be at least as secure as, or increase the security above, the current system for obtaining medical information**
   The use of electronic software to obtain medical information should be at least as secure as the current system or should increase the security of obtaining medical information above that of the current system.

6. **An electronic process must provide an audit trail of the consent process and the data sent, making it available to all parties**
   An electronic process should generate an audit trail that is readily available to both individual and GP. The audit trail should clearly show what consent was granted, by whom, when and why.

7. **An electronic process should conform to ISO/ BSI Standards or equivalent**
   Insurers' electronic processes for obtaining medical information should conform to the minimum ISO/BSI certification standard or demonstrate a similar level of data security in their internal processing.

8. **An electronic process should be compliant with ICO, GMC, and NHS Information Technology guidance and standards and all relevant data transmitted should be encrypted to NHS standards**
   An electronic process will conform to relevant guidance provided by the Information Commissioner's Office (ICO), General Medical Council (GMC) and will meet NHS Information Governance and Technology standards. All data transmitted through an electronic process should be encrypted to NHS standards and transported in a compliant manner.

9. **An electronic process should have undertaken a Privacy Impact Assessment or equivalent**
   Any insurance company introducing an electronic process for obtaining medical information will undertake a Privacy Impact Assessment or equivalent**.** A completed assessment cannot be made public but an insurer should be able to confirm what impact assessment process was used.

10. **An electronic process must enable the Data Controller to provide information to a third party in accordance with Data Protection requirements and make clear the onward use of data**
    The release of information must enable the Data Controller to provide information to a third party in accordance with DPA requirements and consent must be given by the patient to the onward use of data. The process should meet NHS Information Governance standards when producing the report and only permitted users should be able to generate and deliver a report.