Bundesministerium
für Gesundheit
und Soziale Sicherung

Berlin/Bonn, July 2005

The German eHealth Strategy

(Target and strategy, concept, legal framework, activities/roll-out plan, costs and return of investment, European perspective)

1. The healthcare system in Germany is a system with a pressing demand for intensive communication between the different actors with the aim of achieving better collaboration and thus numerous positive results for the health of the citizens, the healthcare system and the State's economic situation. The overall **TARGET** is the modernisation of the healthcare system using information and communication techniques (ICT), in order to:
   - establish more citizen-oriented services,
   - support patient-centred care,
   - improve quality and services,
   - reduce costs,
   - provide better data for health systems management.

   Modernizing the healthcare system is part of the overall strategy towards an Information Society as described in the European Union Lisbon Strategy.

2. The **STRATEGY** for achieving this target is the following:
   - establishing an ICT infrastructure financed by one/a few applications, so that other applications can build on the infrastructure without having those basic costs. Priority applications (having a positive cost-benefit ratio) are:
     - online verification of insurance status (mandatory for citizens),
     - transmission of (drug) prescriptions (mandatory for citizens),
     - drug interaction and contraindication checks (like some of the other envisaged applications, voluntary for the citizens).
   - implementing applications (and functions) of a private electronic patient record and other applications, step by step, using the established infrastructure.

   Having established such applications, data provided electronically can, in principle, be better used for other, different purposes such as reimbursement, studies or statistics.

   However, since data cannot be read from medical application-related storages

(because of citizen-managed/citizen-oriented encryption) at the source of data, separate purpose-related data streams have to be implemented using aggregation, pseudonymisation and anonymisation techniques.

From a **EUROPEAN PERSPECTIVE,** mobile citizens are to be supported in such a way that their local (regional/national) eHealth services can be used abroad. Consequently, collaboration with the other Member States of the European Union on interoperable eHealth infrastructures, services and applications is necessary.

3. The underlying **CONCEPT** is the citizen-managed, personal electronic health record. This personal electronic health record
   - is offered and operated by the healthcare system,
   - is defined by law and by contracts entered into by the self-administered healthcare system on the federal level,
   - the data is normally provided and used by healthcare professionals (in the form of electronic copies of the original documentation), if the citizen gives his consent for an application and to specific healthcare providers,
   - some data might be provided by the citizen himself/herself *('Patientenfach')*,
   - the citizen is the owner of the data (right to delete!).

   For access to the personal electronic health record
   - in principle, a special smart card *('Gesundheitskarte'*, Electronic Health Card) is used as the citizen's tool to manage data in a trustworthy and secure way,
   - in principle, access to the Electronic Health Card – and the managed data stored on it or accessible via a secure network – is open exclusively to authorized healthcare professionals authenticated by means of a Health Professional Card (HPC),
   - in principle, electronic authorisation by the citizen (the insured person) is required (one important exception is access to the voluntary emergency data set).
   - access to the data is logged,
   - the access-rights (read/write/delete!) are managed by the citizen (if desired, on the detail level of data); exceptions are the mandatory data sets such as those for administrative data,
   - data is signed using digital signatures as proof of their completeness and correctness and of the authorship of the data.

   A special infrastructure is constructed by:
   - connecting 'closed virtual private networks' operated by the responsible healthcare organizations/contract partners operating in the healthcare system (sectors: doctors, hospitals, pharmacies, dentists, …),
   - using special 'connectors' to connect local systems to the network, to infrastructure services and to smart card terminals,
   - using cryptographic techniques between infrastructure components for

authentication and encryption/decryption,
- using (qualified) digital signatures,
- storing and transporting data using cryptography, so that the citizen's data can only be used with his/her consent (in principle, a private key stored on the Electronic Health Card must be used by the citizen himself to provide decrypted data).

The storage concept is the following:

- data–and/or copies of the original data–are stored (in principle) by each healthcare provider in a distributed environment,
- some data is stored on the '*Gesundheitskarte'* itself:
  - (European) emergency data/basic clinical data set,
  - identification data,
  - insurance data,
  - private cryptographic keys,
  - some public key certificates.
- citizens can use their own data after authorization by a smart card with a qualified digital signature (might be the Electronic Health Card itself) and if the data has been copied to a special storage space ('*Patientenfach*').

4. The **LEGAL FRAMEWORK** is defined on the federal level in the Social Code V (§§ 290-291).

   The law provides for

   - a new lifelong patient identifier which identifies the citizen, independent of where he/she is insured, for purposes of the healthcare system and
   - the introduction of an Electronic Health Card (*'Gesundheitskarte*') with its applications and functions as the citizen's tool for managing applications and his/her personal medical data sets.

   The law defines mandatory and voluntary applications that can be managed using the '*Gesundheitskarte*' as a tool. The mandatory applications are introduced in the first step; the voluntary applications will be added step by step.

   The mandatory applications are:

   - provision of administrative data (data identifying the citizen and his/her insurance status),
   - provision of information about share of private co-payment,
   - transmission of electronic prescriptions,
   - provision of data supporting European regulations for the exertion of rights for medical treatment in the Member States of the EU (in Germany the data is not only visible but also stored on the chip, thereby creating an 'Electronic European Health Insurance Card').

   To protect citizens' private data, the law describes citizens' rights and means of protecting their data. Citizens' rights and data privacy are legally ensured by:

- the citizen’s consent (to be documented on the Electronic Health Card),
- regulations for logging access (at a minimum the last 50 accesses have to be logged),
- prohibition of non-care related utilization,
- prohibition of confiscation of health-related personal data.

The responsibility for issuing Health Professional Cards ('*Heilberufsausweis*', '*Berufsausweis*') and the confirmation of health professionals has to be defined on the State level ('*Länder*').

The definition, establishment and operation of an interoperable infrastructure is conducted by a specialised company ('gematik', Berlin), owned by all contract partners of the self-administered healthcare system on the federal level.

There is a contract on the federal level about how to finance

- the company: gematik,
- the first infrastructure set-up (definition, test, roll-out) and
- the operation of the infrastructure,

including some special rules on how to finance infrastructure in hospitals.

The financing principle is the following:

- during the definition and test phase, extra charges are paid to the healthcare providers for every reimbursement case,
- during the operating phase extra charges are paid to the healthcare providers every time the infrastructure services are used (transaction charges).

gematik has to define:

- the technical framework and the security concept,
- the content and structure of data records,
- the test and certification procedures for hard and software products or components,

if these are necessary for an interoperable and compatible infrastructure.

gematik is parity financed by insurance funds (45% statutory, 5% private) and healthcare providers. For decisions, a majority of 67% of the shares is required.

The Law provides for an Advisory Board for gematik comprised of representatives of

- the federal states ('*Länder*'): 4,
- patient organisations: 3,
- scientific organisations: 3,
- industry: 3,
- the Federal Commissioner for Data Privacy,
- the Federal Commissioner for Patients' Affairs.

The Federal Ministry of Health has the right to demand the elimination of identified shortcomings in gematik's implementation decisions and to set deadlines. If such deadlines are not met, the Ministry is entitled to make all necessary specifications by ordinance.

5. Since it is not responsible for the implementation of infrastructure, services and

applications–this task being incumbent on the self-administration system by law–the Federal Ministry of Health and Social Security has initiated a number of **ACTIVITIES** to support the process. Development projects made the first contributions towards infrastructure, concepts and architecture:

- the project 'bIT4Health' made a proposal for the definition of a generic component-model framework architecture,
- the project 'Solution Outline' developed a project plan for concept and architecture definition and health card specification,
- a R&D project had the task of defining an open standard architecture for an ehealth telematics platform.

In March 2005 (Cebit), the results of those projects were handed over to the newly founded Society for Telematics ('gematik').

The **ROADMAP** for implementing the applications, functions and services of the Electronic Health Card in Germany is the following:

- pilot tests operating at the regional level ('*Modellregionen*'/'*Testregionen*') are to be adapted to the overall Electronic Health Card concept beginning in the fourth quarter of 2005,
- the preparation for practice tests in selected regions and environments has started ('Mini-tests', field trials),
- the pilot tests have the character of an introduction test with the option for improvements,
- if the set-up of a test is sound and solid, the test will migrate to introduction in the region,
- the gradual implementation of first applications will begin in 2006 and will be carried out on a step-by-step basis
  - by region,
  - by application,
  - by function,
  - by infrastructure service.

6. The central **INFRASTRUCTURE** set-up consists of
   - connected virtual private networks, and
   - special centralized infrastructure services.

   The local infrastructure set-up consists of
   - modernized hard-/software in doctors' offices, hospitals, pharmacies and other locations,
   - special secure connectors to the network and to serve card terminals,
   - smart-card terminals.

   The infrastructure set-up will probably cost about 1 - 1,5 billion euro.

7. The **DEVELOPMENT**/deployment by gematik and the operating centres of the self-administered contract partners of the health system has relevance for:

- legacy systems of the healthcare partners,
- specifications used by industry to construct products,
- product tests and integration tests,
  - functional tests,
  - application tests,
  - laboratory tests of complete scenarios,
  - mini-tests in real environments,
  - field trials ('*Modellregionen*'/'*Testregionen*'),

and probably costs about 100-150 million euro in the timeframe 2004-2007.
The prognosis for the return of investment is a maximum of 3 years depending on the degree to which voluntary applications are used.