

Taiwan's Health IC Smart Card Security and Privacy Policy

translated by Yuh-Ning Chen PhD, [MartSoft Corp.](#)

(I) SYSTEM SECURITY POLICY

(1) Contractual restriction

The contract between the Bureau of National Health Insurance (BNHI) of Taiwan and its general contractor TECO includes the following items:

General contractor and its employees can't disclose any proprietary information of BNHI. BNHI also requires general contractor's employees and the subcontractors to keep the contractual agreement confidential;

During the effective time of the contract, if contract signing parties disclose any information on the Health IC card or any information about the card holders, BNHI can take away the deposit and terminate part of or the full contract, and the violator would pay a penalty fee;

If any of the Health IC card, security modules, reader systems, application systems, software or hardware is provided by foreign entities, the authorization document from the foreign companies and the necessary validation and certification documents should be provided.

(2) System security proposal

BNHI requests contractors to provide a total system security policy for a complete management mechanism. For this rule, contractors should provide documents such as "System Security proposal", "System Security mechanism design document" and "System Security policy management user's handbook" for experts approval and for execution.

(3) Establish the health IC card information security protection team

To prevent improper usage and leakage of information of the health IC card, BNHI establishes the health IC card information security protection team. This team will guard all relevant security issues.

(II) PROTECTION OF INDIVIDUAL INFORMATION AND PRIVACY RIGHT

(1) Privacy Policy

(1a) The personal information is used for health insurance and medical services only.

Health IC [smart card](#) is used for identification purpose to provide the correct medical service to the right person. It will not provide usage beyond health management and clinical services.

(1b) The health IC [smart card](#) does not store the full patient health/treatment information.

The current patient information stored on the health IC [smart card](#) only includes what's originally on the paper card; it does not involve patient privacy. Some people are very concerned about whether a smart card could violate the cardholder's privacy. BNHI has already established open communication platform with human right and patient activist groups. The communication is ongoing; therefore to plan for addition of future prescription and clinical treatment and test information on the smart cards, people can advocate their right of health card knowledge and self-management. The private medical history record that everyone is concerned about will be stored in each hospital/clinic. There is only 32K of memory on the smart card; it is not sufficient to store all patient record and test image information. The only accepted items on the smart card are for improving the quality of the treatment, and reducing the cost of patient information processing.

(2) Smart card operation security and privacy

(2a) High grade card printing to prevent counterfeiting

Special printing designs including guilloche, rainbow printing, microline printing, optically variable ink printing are used. Ultraviolet fluorescent printing is used for the high-end security. Background of the photo is processed to protect against counterfeiting. The security of the card is comparable with that of the credit cards.

(2b) Privacy is protected through multiple security mechanisms.

(i) Information stored on the [smart card](#) is encrypted.

(ii). Each BNHI IC card reader must have a SAM Card (Security Access Module), which is issued by the BNHI to verify the identity of healthcare provider. Data stored on the cards cannot be read without going through a strict authorization and mutual authentication process. Besides, there will not be any medical history recorded on the BNHI IC Card.

(iii). Healthcare Professional Card will be issued as a further use of BNHI IC Card. Healthcare providers can access the medical information on the IC chip and write appropriate information to the card only through the Healthcare Professional Card.

(iv). Cardholders can set up their own personal identification number (PIN) for their cards at the BNHI's Kiosk (one kind of the readers) to protect their information. This personal identification number has higher privilege than a healthcare professional. The healthcare professional can't read beyond the basic medical information without cardholder's input of the pin number.

(3) Security of information communication

(i) Adopt the highest standard for security control: three layers of firewalls are installed; hacker intrusion drills are performed at irregular intervals to detect possible security weaknesses. If hacker intrusion is found, there will be immediate change of keys.

(ii). Adopt the close loop VPN that does not connect with the Internet, so invasion of the hackers can be avoided. In the same time, VPN's are networked therefore Chunghwa telecom co ltd (Taiwan's largest electricity and telecom company) and its subsidiaries can support each other. The network bandwidth can adjust automatically to ensure the quality of communication and reducing the traffic jam in the Internet.

(iii). Use encoding in transmission. IC [smart card](#) only store necessary prescriptions for chronic disease, and certain disease names or expensive exam. Each item is transmitted through code, not in Chinese.

(4) Prevention of computer virus

(i) BNHI utilizes the best practice in virus prevention mechanism.

(ii) BNHI encourages end users to adopt antivirus protection software:

- a. Main terminals provide end users antivirus protection program renewal capability.
- b. Establish gateways with antivirus protection companies, e.g. Trend, Norton etc.
- c. BNHI advocate the adoption of antivirus protection softwares.

(5) Crisis management and response plan

Research and design crisis management plan; clarify crisis type, levels, and recognition of the crisis and symptoms at the onset of the crisis. BNHI also organizes a crisis management team to deal with emergency and crisis prevention. There will be established reaction procedures for emergencies like natural disaster, electricity outage etc;

(i) If the smart card is stolen or lost, the corresponding card file is destroyed immediately.

(ii) UPS (uninterruptible power supply) are installed to prevent the damage of large-scale electricity outage: if such outbreak does occur, system can be shut down properly to prevent the lost or damage of hardware and software.

- (iii) Three layers of firewalls are installed; VPNs are not connected with the Internet, hacker intrusion drills are performed at irregular intervals to detect possible security weaknesses. If hacker intrusion is found, there will be immediate change of keys to prevent further intrusion.
- (iv) There are different levels of authorization for staff to access the data. There will be an audit trail for data access to prevent breach of privacy and sharing of privileged information.

[End]

Note: This article can be found in <http://www.enhi.com.tw/> . It describes the basic policies and operations of the HIPAA equivalent in Taiwan [Smart Card](#) project- an example of a most recent successful large-scale health care smart card project. The translator believes that this translation would provide clear and convincing evidences why smart card is a major and necessary part in enforcing HIPAA act. Without smart cards, there will not be sufficient privacy and security as required by HIPAA act.