Surface mail services to Iran temporarily suspended

Hongkong Post announced today (November 14) that, due to disruption of sea transportation services, all surface mail services (including letter post items and parcels) to Iran are suspended with immediate effect until further notice.

LCQ6: Hospital accreditation programme

Following is a question by the Professor Hon Joseph Lee and a reply by the Secretary for Food and Health, Professor Sophia Chan, in the Legislative Council today (November 14):

Since 2009, the Hospital Authority (HA) had implemented a hospital accreditation programme (the accreditation programme) by phases in public hospitals, with a view to enhancing the accountability of hospitals for service quality and safety. Some healthcare workers have relayed that while the accreditation programme put much emphasis on the procedure, it disregarded the manpower shortage problem (i.e. the so-called "accrediting the procedure but not the manpower"). Healthcare workers were worn out by the large amount of paperwork generated by the accreditation programme, which conversely affected the quality of clinical services. After discussing with the Secretary for Food and Health, HA decided in January this year to suspend the accreditation work, so as to alleviate the work pressure on healthcare workers during the influenza surge and to allow them more time for taking care of patients. It has been reported that HA suddenly terminated the accreditation programme last month and indicated that it was exploring a new model for implementing the accreditation programme. In this connection, will the Government inform this Council whether it knows:

(1) the details of the new accreditation programme to be implemented, including the implementation date, the expenditure and manpower involved, as well as how the accreditation of both the procedure and manpower will be achieved; and

(2) how HA will ensure that the implementation of the new accreditation programme will neither increase the work pressure of healthcare workers nor affect the quality of healthcare services?

Reply:

President,

My consolidated reply to the various parts of the question raised by the Professor Hon Joseph Lee is as follows:

It is one of the key strategic directions of the Hospital Authority (HA) to ensure patient safety and improve patient services. Given the advancement in medical technology, population growth and increasing complexity of hospital services, the establishment of a sound risk and quality management system has become fundamental to improving the quality of healthcare services. Hospital accreditation is a general global trend. It has been widely adopted across the world to enhance the quality of healthcare facilities and ensure patient safety. Through hospital accreditation, the risks and inadequacies of such aspects as hospital management, facilities and operation are assessed in an objective and systematic manner to ensure continuous service quality improvement.

The HA launched the Hospital Accreditation Programme (the Programme) in 2009. With the concerted efforts of hospitals and their staff over the years, 20 HA hospitals have been awarded full accreditation status as at 2016. Drawing from the experience of implementing the Programme in the past few years, and on the advice of frontline staff and stakeholders, the HA initiated a comprehensive review of the Programme in February 2017. In mid-July 2017, having regard to the sharp increase in demand for public hospital services during the influenza summer surge and the work pressure on frontline staff, the HA suspended all hospital accreditation activities. During the suspension period, the HA continues to explore ways to enhance the continuous quality improvement model taking account of local situation and characteristics.

In the review process, staff members agreed that the main purpose of hospital accreditation was to establish a sound risk and quality management system to ensure continuous quality improvement. Over the past few years, HA hospitals have effected improvements as appropriate in various areas and services on the basis of the recommendations of self-evaluations and independent surveyors. For example, sterilising facilities in operating theatres and their operation are improved, medication safety is enhanced and occupational safety and health of their staff are further strengthened. Staff members also expressed during the review that they had been worried and concerned about the implementation of hospital accreditation. For example, certain accreditation standards and improvement recommendations might not be suitable for adoption in public hospitals; preparation for accreditation and survey documents generated extra work pressure on staff; and there were variations in surveyors' rating standard and their experience.

At present, a new working group, comprising representatives from the HA Head Office and hospital clusters, has been set up by the HA to explore how to draw up a new continuous quality improvement plan for public hospitals. The directions to be considered will focus on the following:

(1) To carry out improvement work at a steady pace with emphasis placed on continuous quality improvement and patient safety, rather than on performance assessment of individual units or staff members or enforcement of requirements under the accreditation standards for enforcement's sake.

(2) To eliminate duplication of work processes, including reducing paperwork as well as the frequency of hospital visits and ward rounds. The HA may allocate extra resources to help hospital clusters handle the work for continuous quality improvement, so that frontline healthcare staff can focus on their routine clinical and healthcare duties. The elements of continuous quality improvement may also be integrated into routine clinical and healthcare services, so as to spare the staff the need to undergo extra training.

(3) To enhance the support of HA Head Office for hospital clusters. The HA Head Office may take up the responsibility of organising, implementing and co-ordinating continuous quality improvement programmes. The HA may also co-ordinate the deployment of extra resources for carrying out patient or staff safety improvement measures identified during the implementation of continuous quality improvement programmes.

The support and collaboration of every staff member are necessary for enhancing continuous quality improvement. Currently, the HA is preparing to organise consultation sessions and focus groups for staff of different grades to enhance staff communication and collect their views. The HA will also invite patient groups and stakeholders to give their views on the new continuous quality improvement plan through different channels.

The HA will continue to explore how to draw up a new continuous quality improvement plan taking into account local situation and characteristics as well as the views of different stakeholders, so as to provide patients with quality and safe healthcare services.

LCQ15: Employment visas for personnel of Taipei Economic and Cultural Office

Following is a question by the Hon Lam Cheuk-ting and a written reply by the Secretary for Constitutional and Mainland Affairs, Mr Patrick Nip, in the Legislative Council today (November 14):

Question:

It has been reported that the former Director General of the Taipei Economic and Cultural Office (TECO) (the Taiwan authorities' representative office in Hong Kong) left Hong Kong at the end of July this year upon completion of his term of office, and his successor has so far been unable to come to Hong Kong to take office because he has not been granted an employment visa by the Hong Kong Special Administrative Region (SAR) Government. In this connection, will the Government inform this Council:

(1) whether the SAR Government is required to consult the Central Authorities

beforehand on matters relating to the granting of employment visas to TECO's personnel; if so, of the details;

(2) whether it has explained to the Taiwan authorities why it has not granted an employment visa to the Director General – designate of TECO; if not, of the reasons for that; and

(3) whether it has assessed the impacts of leaving the office of TECO's Director General vacant for several months on (i) the operation of TECO, (ii) the economic, trade and cultural exchange activities between Taiwan and Hong Kong, and (iii) the relationship between the authorities of both places; if it has assessed, of the outcome; if not, whether it will conduct such an assessment expeditiously?

Reply:

President,

Our consolidated reply to Hon Lam's question, after consulting the relevant bureaux, is as follows:

The economic, trade and cultural exchanges between Hong Kong and Taiwan have all along been ongoing. Last year, Taiwan was Hong Kong's third largest trading partner and Hong Kong was Taiwan's fourth largest trading partner; there were also over two million visitor arrivals from Taiwan, which was Hong Kong's second largest visitor source market after the Mainland. Meanwhile, arts groups in the local communities of Hong Kong and Taiwan also visit one another from time to time. The Hong Kong Week, which aims to showcase the cultural characteristics of Hong Kong, has been held in Taiwan for six years.

In 2010, the Hong Kong-Taiwan Economic and Cultural Cooperation and Promotion Council (ECCPC) and the Taiwan-Hong Kong Economic and Cultural Co-operation Council (THEC) were established in Hong Kong and Taiwan respectively to promote exchanges and co-operation between the two places. Achievements have been made in various areas. We will continue to foster economic, trade and cultural exchanges and co-operation between Hong Kong and Taiwan through the ECCPC-THEC platform in a pragmatic manner.

The Hong Kong Special Administrative Region Government will not comment on individual cases or make public information concerning individual cases. In handling each application, the Immigration Department acts in accordance with the laws and policies, and decides whether to approve or refuse the application after careful consideration of circumstances of each case.

Fraudulent websites related to The

Shanghai Commercial & Savings Bank, Ltd.

The following is issued on behalf of the Hong Kong Monetary Authority:

The Hong Kong Monetary Authority (HKMA) wishes to alert members of the public to a press release issued by The Shanghai Commercial & Savings Bank, Ltd. on fraudulent websites, which has been reported to the HKMA. Hyperlink to the press release is available on the HKMA website for ease of reference by members of the public.

Anyone who has provided his or her personal information to the websites concerned or has conducted any financial transactions through the websites should contact the bank concerned using the contact information provided in the press release, and report to the Police or contact the Cyber Security and Technology Crime Bureau of the Hong Kong Police Force at 2860 5012.

LCQ2: Enhancing information security and the protection for privacy of personal data

Following is a question by the Hon Charles Peter Mok and a reply by the Secretary for Constitutional and Mainland Affairs, Mr Patrick Nip, in the Legislative Council today (November 14):

Question:

In recent years, incidents involving massive leakage of personal data by government departments and private organisations have occurred frequently. Not until half a year after learning of the leakage of the data of about 9.4 million passengers did an airline announced it last month. In addition, in less than a month after the launch of the Faster Payment System, a number of fraud cases occurred in which the fraudsters committed crimes by making use of the personal data of members of the public and taking advantage of the loopholes in the process of setting up direct debit authorisation by electronic wallets users, thereby causing financial losses to the members of the public. On enhancing information security and the protection for privacy of personal data, will the Government inform this Council:

(1) whether it will, by making reference to the General Data Protection Regulation of the European Union, study prescribing in the Personal Data (Privacy) Ordinance the obligations of data processors, and that data users

are required, in the event of data leakage incidents, to notify the Office of the Privacy Commissioner for Personal Data and the data subjects within specified time limits; and

(2) whether it will comprehensively assess the information security risks currently faced by government departments, industries such as finance and telecommunications as well as public utilities, formulate a cross-sector information security strategy, and step up the training for information security talents (e.g. by setting up a specialised college)?

Reply:

President,

Regarding the respective parts of the question raised by Hon Charles Mok on enhancing the protection of personal data privacy and capability of responding to information security risks, our reply in consultation with the Innovation and Technology Bureau (ITB) and the Security Bureau (SB) is as follows:

(1) The Personal Data (Privacy) Ordinance (PDPO) was enacted in 1995 and has been in operation since 1996. Subsequent to the public consultation on the PDPO and the relevant legislative amendments conducted by the Government between 2009 and 2010, the Personal Data (Privacy) (Amendment) Bill was introduced in the Legislative Council (LegCo) in 2011 and was passed by LegCo in June 2012.

During the above-mentioned consultation exercise on the PDPO, one of the issues for consultation was the personal data breach notification system. The primary consideration on the issue back then was whether a notification system should be instituted to require relevant organisations to notify the Office of the Privacy Commissioner for Personal Data (PCPD) and the affected individuals in the event of a personal data leakage, so that they could take measures to mitigate the risks posed by the data leakage, and whether the notification system should be voluntary or mandatory. Of the public views received, about half were in support of a voluntary notification system, while around one-quarter favoured a mandatory notification system. Respondents who supported a voluntary system considered that a mandatory system would impose undue burden on data users. Taking into consideration the possible impact of implementing a mandatory notification system, the Government decided to start with a voluntary notification system. To assist data users in giving data breach notifications, the PCPD issued the "Guidance on Data Breach Handling and the Giving of Breach Notifications" (Guidance) in June 2010, and subsequently made amendments to the Guidance in October 2015. The Guidance issued by the PCPD provides guidance and assistance to data users on the steps to be taken in handling data breaches. A data breach notification form is also attached to the Guidance to make it more convenient for data users to give notifications.

The Government and the PCPD noted that in the light of rapid development and wide use of technology in recent years, the processing of personal data has become massive and digitalised, resulting in higher risk posed to data

users and owners as the amount of data involved in personal data leakage incidents has increased. There are views that this Cathay Pacific incident has revealed that there is room for refining and enhancing the PDPO. In this connection, the Constitutional and Mainland Affairs Bureau will keep close watch on the PCPD's investigation results and recommendations regarding the incident. Meanwhile, we have started a review in collaboration with the PCPD on the stipulations and penalties under the PDPO. While noting that there are views calling for the requirement for data users to give timely notification in data breach incidents, we are also aware of concerns in some quarters on how "data breach" should be defined, as well as the compliance capability and operational costs of businesses. We will examine carefully how the regulation of data protection and the notification arrangements could be enhanced.

(2) To protect government's information systems and data assets, having made reference to international standards, the Office of the Government Chief Information Officer (OGCIO) has formulated a comprehensive set of "Government IT Security Policy and Guidelines" (Policy & Guidelines) which covers many different aspects including security requirements for information security management framework and human resources, protection and encryption requirements for information systems and data assets, connection and access control, network and outsourcing service security, incident response and recovery, etc. OGCIO will conduct regular audits to ensure that all departments comply with the Policy & Guidelines, as well as review and update the Policy & Guidelines from time to time to address the ever-changing cyber threats.

For infrastructure facilities owned by key industries and organisations and those not owned by government, the relevant regulatory bodies will formulate regulatory measures. In view of their unique business nature, the information security strategy, incident response and business recovery arrangements formulated by different industries vary. Industries can make reference to the Policy & Guidelines available at OGCIO's website in developing information security policies and measures that meet their needs. When necessary, OGCIO will also exchange views with the relevant regulatory bodies and give advice.

Furthermore, OGCIO, the Cyber Security and Technology Crime Bureau (CSTCB) under the Hong Kong Police Force and the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) work closely to provide cyber security related information and support to different stakeholders including government departments, key industries and organisations, and the general public, as well as publish information on major incidents and recommend preventive and remedial measures. To prevent and combat technology crimes, CSTCB has been dedicated to help enhancing critical infrastructure operators' awareness to cyber security, and their capability in handling cyber security incidents; and conducting timely cyber threat audits and analyses so as to prevent and detect cyber attacks on critical infrastructure.

For the industries, HKCERT works with industry associations to promote cyber security awareness and best practices in different sectors, as well as provide public and private organisations and the public with news on information security incidents, guidelines for defence against cyber threats

and support services. OGCIO also implements the cross-sector "Cyber Security Information Sharing Collaborative Platform" to exchange information with public and private organisations as well as cyber security experts, and share risk mitigation measures, so as to more effectively enhance the overall cyber security in Hong Kong. CSTCB has also been hosting quarterly cyber security seminars to strengthen the overall defensive capabilities of such service sectors as banking and finance, transport and aviation, communications, public utility and government services in handling cyber security incidents.

Since 2014, the CSTCB has been conducting various types of cyber security drills together with industry stakeholders and local critical infrastructures. Through various simulated incident scenarios, cyber security drills test the capabilities of incident analysis, the standing incident response procedures and the communication protocol of the participants. The simulated cyber attacks incidents include the common scenarios with profound impacts, such as distributed denial-of-service attacks, web defacement, intrusion of network and information systems, ransomware, malware and sensitive data breaches. In addition, CSTCB co-organised in January 2018 the second Inter-departmental Cyber Security Drill with the Government Computer Emergency Response Team Hong Kong, in which 40 government bureaux and departments, through different scenarios of simulated cyber attacks, strengthened their cooperation in cyber security and capabilities in emergency response.

On education work, OGCIO and CSTCB also join hands with HKCERT to proactively promote the nurturing of talents in cyber security professionals, and co-organise activities with different organisations, such as the Cyber Security Professionals Award, cloud security professional certification seminars and Information Security Summit to enhance the information security knowledge and skills of IT practitioners. The Government also encourages tertiary institutions to strengthen information security modules in their IT-related programmes, and promote information security education in primary and secondary schools to cultivate the youth's interest in and concern about information security.

Thank you, President.