Bills Committee on
Electronic Health Record Sharing System Bill

The Administration's Response to the follow-up issues arising from the discussion at the meeting on 26 May 2014
(Other follow-up issues)

This paper sets out the Administration's response to other follow-up issues arising from the discussion at the meeting of the Bills Committee on the Electronic Health Record Sharing System (eHRSS) Bill on 26 May 2014.

(a) Response to other issues of concern raised by the deputations

Definition of healthcare professionals

2. We consider that the definition of healthcare professionals should cover all the 13 statutorily registered healthcare professions. They are: pharmacists, dentists, dental hygienists, medical practitioners, midwives, nurses, medical laboratory technologists, occupational therapists, optometrists, radiographers, physiotherapists, chiropractors and Chinese medicine practitioners (CMPs) within the meaning of respective ordinances / regulations. In general, their professional conduct is subject to the regulation of the respective registration boards and councils. The registration status of individual professionals is also verifiable. The 13 statutorily registered professions are listed in the Schedule of the bill. Pursuant to clause 60 of the bill, the Secretary for Food and Health (SFH) may by notice published in Gazette amend the Schedule in the future.

Participation of CMPs

3. We noted the supportive views for CMPs to participate in eHRSS. As aforementioned, CMPs have already been included in the schedule of healthcare professionals in our bill. To facilitate CMPs to later take part in the sharing process, we will continue to work with the

CMP sector on the standardisation of Chinese medicine (CM) terminologies and improving the technical readiness of CMPs. On the former, we have provided funding for the Hospital Authority (HA)'s CM Division to carry out the CM Data Standardisation project during Stage One of the eHRSS Programme. We will continue to implement the project. On the latter, we will provide funds to HA to develop an all-in-one CM clinical management system suitable for adoption by CMPs in the private sector.

<u>eHR data used for research</u>

4. Data in eHRSS will be valuable for research and statistical purposes relevant to public health or public safety. At the same time, the Administration acknowledges the need to strike a balance between the public interest in conducting research and protecting privacy of the participating patients. We have set out a due process to consider applications for such uses in Divisions 2 and 3 of Part 3 of the Bill.

5. Any application for uses of electronic health record (eHR) for research would require the submission of a written proposal setting out the nature and objectives, the anticipated public or scientific benefit and any other information specified by the Commissioner for the eHR (eHRC). Applications for use of non-identifiable data will be considered by the eHRC, while those for use of identifiable data will be considered by SFH. The eHR Research Board established under clause 53 would assess the applications involving identifiable data and provide SFH with recommendations on whether to approve or refuse the applications, and the approval conditions. The approval conditions may include special requirements on safeguarding privacy. As provided in clause 45 of the Bill, a person commits an offence if the person knowingly contravenes a condition for use of the eHR data for researches and statistics imposed under clause 32(1)(a).

6. One deputation raised concern on data re-identification risk as anonymized data cannot be assumed to be privacy safe. We note that simply removing the personal identifiers such as name, Hong Kong

Identity Card, etc. may not be able to completely de-identify certain medical records. In fact, as provided in clause 2(2) of the Bill, any data or information of a healthcare recipient (HCR) is non-identifiable data if the identity of the HCR is unascertainable from the data or information. Fulfilling the requirements in the Bill in relation to non-identifiable data will involve more than merely removing the personal identifiers of a particular record. In the process of the de-identification, careful review of the record will be conducted to remove any data that will pose the risk of re-identification as far as possible.

Software market of clinical management systems

7. The Government's policy is to maintain a level playing field for all clinical management systems (CMS) to connect to the eHRSS. The purpose of providing Government-developed software i.e. CMS on-ramp is to provide a low investment means for healthcare providers (HCPs) to connect to eHRSS. Use of Government software is not mandatory. HCPs may choose to deploy clinical software/system suitable for their own operational needs or deploy CMS on-ramp and add value-adding operational features. We will provide information on data sharing standards, interface specifications and interoperability requirements to facilitate those private hospitals and clinics using non-government developed systems for eHRSS connection. For popular systems in the market used by private clinics, we have been working very closely with vendors/providers to discuss their connectivity to eHRSS. Action plans have been formulated for certain common commercial systems and also the CMS 3.0 of the Hong Kong Medical Association, the Dental Clinic Management System of the Hong Kong Dental Association, CMS of the University Health Service of Hong Kong Polytechnic University, etc.

Fees for DARs

8. There is concern about the fees charged on HCRs making a Data Access Request (DAR). According to the Personal Data (Privacy) Ordinance (Cap. 486) (Privacy Ordinance), a data subject can request a copy of the personal information hold by the data users. The Privacy

Ordinance also specifies that the data user may charge a fee which is not excessive to comply with a DAR. Given that the information stored in eHRSS is in electronic format, we anticipate that the DAR fee for data stored in eHRSS will not be substantial.

Patient Portal

9. Several deputations have expressed the view in support of the provision of a patient portal in Stage Two to facilitate patients to access their data. We have undertaken to conduct a study on whether and how to provide for a patient portal in Stage Two of the eHRSS.

Training for IT sector / HCPs

10. The engagement and participation of private healthcare and IT service providers are essential to the success in building up the eHRSS. We have launched a Service Provider Training Scheme to equip interested IT vendors with necessary knowledge to provide end-user support services to HCPs on CMS On-ramp installation. In addition, we plan to conduct seminars/briefings to interested HCPs to assist them in adopting CMS on-ramp upon the commencement of the eHRSS. We are also working closely with the IT sectors to discuss connectivity of other clinical management softwares to eHRSS.

Other views expressed

11. The other views expressed are mainly related to requests for more involvement and engagement of stakeholders, avoiding delay of the eHRSS project schedule, enhancing user-friendliness of the eHRSS and minimizing additional workload for front-line staff. The Administration is grateful for these views and will take them into consideration in designing our subsequent work plans.

(b) Request by HCRs not to upload certain health information

12. Before a registered HCP provides the health information of a

particular HCR to the eHRSS for sharing, he must first obtain the HCR's sharing consent. The HCP must also have an electronic medical record (eMR) system of its own to keep the medical record of its own patients. That eMR system must be eHR-compliant to enable health data in particular format to be transmitted to the eHRSS. When a doctor starts inputting HCR's information into the HCP's own eMR, and with the HCR's sharing consent, those data within the sharable scope will be uploaded to the eHRSS.

13. There is suggestion that an HCR should have the right to request the concerned HCP not to provide certain health information to the eHRSS. In practice, we envisage that the HCP may or may not enter the HCR's certain information into the HCP's own eMR, subject to the professional judgment of the HCP on whether the HCR's request should be acceded to. If certain information is not entered into the HCP's own eMR system, then it will not be uploaded to the eHRSS.

(c) DAR by mentally incapacitated persons

14. There is a question on whether a mildly mentally handicapped person (MIP) would be classified as mentally incapacitated as defined by section 2(1) of the Mental Health Ordinance (Cap.136), and if not, how these mildly mentally handicapped HCR would be able to make a DAR for their health records in the eHRSS.

15. Under section 2 of the Mental Health Ordinance, the term "mentally incapacitated" is construed with reference to "mental incapacity" which is defined to mean "mental disorder" or "mental handicap". The term "mental handicap" is defined as "sub-average general intellectual functioning with deficiencies in adaptive behavior". Accordingly, a "mildly mentally handicapped" person, with deficiencies in adaptive behavior, should fall within the scope of the defined meaning of a "mentally handicapped" person under the Mental Health Ordinance.

16. According to clause 38 of the eHRSS Bill, a "relevant person" as defined in section 2 of the Privacy Ordinance (with the exception of "a

person authorized in writing" by the data subject) may make a DAR or data correction request (DCR) on behalf of the data subject. In the case of an MIP, the guardian[1] may make a DAR or DCR on his/her behalf. However, it is not a must that the DAR/DCR will have to be made by a guardian. According to section 18 of the Privacy Ordinance, the data subject himself/herself, whether he/she is a mentally incapacitated within the meaning of section 2 of the Mental Health Ordinance or not, can make a DAR or DCR himself/herself.

17. In practice, we would foresee that some mildly MIPs, who may not have a guardian appointed, may be accompanied or assisted by others (e.g. family members) in making a DAR or DCR himself/herself.

(d) Composition of the eHR Research Board

18. Clause 54(2) of the bill stipulates that the Research Board is to consist of the following members—

(a) the Permanent Secretary for Food and Health (Health), as ex officio member and chairman;
(b) the eHRC, or a person nominated by the Commissioner as representative, as ex officio member; and
(c) not more than 10 other members appointed by the Secretary for Food and Health.

19. With regard to (c), we consider that the members with different background and expertise could assist in considering different types of research proposals. When drafting this provision, we consider it difficult to predict the number and nature of the research applications to

[1] According to section 2(1) of the Privacy Ordinance, it refers to –

(i) A person appointed under section 44A, 59O or 59Q of that Ordinance to be the guardian of that individual; or

(ii) If the guardianship of that individual is vested in, or the functions of the appointed guardian are to be performed by, the Director of Social Welfare or any other person under section 44B(2A) or (2B) or 59T(1) or (2) of that Ordinance, the Director of Social Welfare or that other person

be received. The mix of expertise required may change over time. We therefore have not prescribed in the Bill the composition or background of the "10" members to allow flexibility.

20. However, we note that some deputations have expressed concern over the composition of the board. To address this issue, the Administration is prepared to consider elaborating on the specific requirements for (c). For examples, we will state that members should include people with experience and expertise in the healthcare, privacy protection, statistics, research, law and information technology. We may also include representative of patient groups and HCPs. We will consider a suitable Committee Stage Amendment to this effect.

(e) New offences under eHRSS Bill and offences in existing ordinances

21. A summary table of new offences under the bill (under Part 5 – clauses 41-46) is at **Annex 1**. A summary table of offences in the Privacy Ordinance and other ordinances that we have made reference to in considering the new offences under the bill are at **Annexes 2 and 3** respectively.

Food and Health Bureau
10 June 2014

Annex 1

New offences under the Electronic Health Record Sharing System Bill (under Part 5 – Clauses 41-46)

Clause	Offence	Penalty
41 (Offences relating to accessing, damaging or modifying data or information)	Knowingly causes a computer[1] to perform a function so as to obtain unauthorized access[2] to data or information in an electronic health record	Liable on summary conviction to a fine at level 6 ($50,001 to $100,000)
	Without lawful excuse, knowingly damages data or information in an electronic health record	Liable on summary conviction to imprisonment for 2 years
	Knowingly - (i) causes access to an electronic health record; (ii) causes modification of data or information in an electronic health record; or (iii) causes impairment to the accessibility, reliability, security or process of an electronic health record; and causes the access, modification or impairment – (i) with intent to commit an offence; (ii) with a dishonest intent to deceive; (iii) with a view to dishonest gain[3] for themselves or for another; or (iv) with a dishonest intent to cause loss[4] to another whether on the same occasion as the person causes the access, modification or impairment or on any future occasion	Liable on conviction on indictment to imprisonment for 5 years

[1] A computer means a device for storing, processing or retrieving data or information.

[2] Access by a person to data or information is unauthorized if—
(a) the person is not entitled to control that access;
(b) the person has not been authorized by another person who controls that access to obtain that access;
(c) the person does not believe that the authorization has been given; and
(d) the person does not believe that, even if the person had applied to the appropriate authority, the authorization would have been given.

[3] A reference to gain includes (i) a gain in money or other property; (ii) a temporary gain or permanent gain; (iii) a gain by keeping what one has; and (iv) a gain by getting what one has not.

[4] A reference to loss includes (i) a loss in money or other property; (ii) a temporary loss or a permanent loss; (iii) a loss by getting what one might get; and (iv) a loss by parting with what one has.

Clause	Offence	Penalty
42 (Offences relating to impairment to System)	Knowingly impairs the operation of the System	Liable on conviction on indictment to imprisonment for 10 years
43 (Offences relating to data access requests and data correction requests)	With intent to evade a data access request or data correction request in relation to any data or information in an electronic record – (a) alters, falsifies, conceals or destroys the data or information; or (b) directs another person to do anything mentioned in paragraph (a)	Liable on summary conviction to a fine at level 6 ($50,001 to $100,000)
44 (Offences relating to untrue statements)	Knowingly makes an untrue statement to enable the person to give a joining consent or sharing consent	Liable on summary conviction to a fine at level 6 ($50,001 to $100,000)
45 (Offences relating to contravening conditions for research or statistics purpose)	Knowingly contravenes a condition imposed under section 32(1)(a)[5]	Liable on summary conviction to a fine at level 6 ($50,001 to $100,000)
46 (Offences relating to direct marketing[6]) [7]	Uses another person's data or information contained in an electronic health record, or a copy (in whatever format) of the data or information, for direct marketing	Liable on conviction on indictment to a fine of $500,000 and to imprisonment for 3 years
	For gain, the person provides to others another person's data or information contained in an electronic health record, or a copy (in whatever format) of the data or information, for direct marketing	Liable on conviction on indictment to a fine of $1,000,000 and to imprisonment for 5 years
	Not for gain, the person provides to others another person's data or information contained in an electronic health record, or a copy (in whatever format) of the data or information, for direct marketing	Liable on conviction on indictment to a fine of $500,000 and imprisonment for 3 years

[5] Section 32(1)(a) refers to the conditions of approval for research or statistics purpose

[6] "Direct marketing" has the meaning given by section 35A(1) of the Personal Data (Privacy) Ordinance (Cap. 486)

[7] This clause does not apply in relation to the use or provision of data or information contained in an electronic health record, or a copy (in whatever format) of the data or information, by a person if, not for gain, the person uses or provides the data or information, or the copy, for a purpose of the offering, or the advertising of the availability, of—
(a) social services run, subvented or subsidized by the Social Welfare Department;
(b) healthcare services provided or administered by the Department of Health or the Hospital Authority; or
(c) any other social or healthcare services that, if not provided, would be likely to cause serious harm to the physical or mental health of (i) the individual to whom the services are intended to be provided; or (ii) any other individual.

Annex 2

Relevant offences in existing laws

Existing offences in the Personal Data (Privacy) Ordinance (Privacy Ordinance) (Cap. 486)

Section	Offence	Penalty
18 (Data access request)	Supplies any information which is false or misleading in a material particular for the purpose of having the data user- (i) inform the person whether the data user holds any personal data which is the subject of the request (ii) if applicable, supply a copy of the data	Liable on conviction to a fine at level 3 ($5,001 to $10,000) and to imprisonment for 6 months
22 (Data correction request)	A person who, in a data correction request, supplies any information which is false or misleading in a material particular for the purpose of having the personal data corrected as indicated in the request	Liable on conviction to a fine at level 3 ($5,001 to $10,000) and to imprisonment for 6 months
35C (Data user to take specified action before using personal data in direct marketing)	Subject to section 35D, a data user who uses a data subject's personal data in direct marketing without taking each of the actions specified in subsection (2) commits an offence. Subsection (2) stipulates that the data user must— (a) inform the data subject— (i) that the data user intends to so use the personal data; and (ii) that the data user may not so use the data unless the data user has received the data subject's consent to the intended use; (b) provide the data subject with the following information in relation to the intended use— (i) the kinds of personal data to be used; and (ii) the classes of marketing subjects in relation to which the data is to be used; and (c) provide the data subject with a channel through which the data subject may, without charge by the data user, communicate the data subject's consent to the intended use.	Liable on conviction to a fine of $500,000 and to imprisonment for 3 years
35E (Data user must not	A data user who has complied with section 35C must not use the data subject's personal	Liable on conviction to a fine of

Section	Offence	Penalty
use personal data in direct marketing without data subject's consent)	data in direct marketing unless— (a) the data user has received the data subject's consent to the intended use of personal data, as described in the information provided by the data user under section 35C(2)(b), either generally or selectively; (b) if the consent is given orally, the data user has, within 14 days from receiving the consent, sent a written confirmation to the data subject, confirming— (i) the date of receipt of the consent; (ii) the permitted kind of personal data; and (iii) the permitted class of marketing subjects; and (c) the use is consistent with the data subject's consent. A data user who contravenes the above commits an offence.	$500,000 and to imprisonment for 3 years
35F (Data user must notify data subject when using personal data in direct marketing for first time)	A data user must, when using a data subject's personal data in direct marketing for the first time, inform the data subject that the data user must, without charge to the data subject, cease to use the data in direct marketing if the data subject so requires. A data user who contravenes the above commits an offence.	Liable on conviction to a fine of $500,000 and to imprisonment for 3 years
35G (Data subject may require data user to cease to use personal data in direct marketing)	A data subject may, at any time, require a data user to cease to use the data subject's personal data in direct marketing. A data user who receives a requirement from a data subject must, without charge to the data subject, comply with the requirement. Failure to comply with the requirement is an offence.	Liable on conviction to a fine of $500,000 and to imprisonment for 3 years
35J (Data user to take specified action before providing personal data)	A data user who intends to provide a data subject's personal data to another person for use by that other person in direct marketing must take each of the actions specified in subsection (2) i.e. the data user must— (a) inform the data subject in writing— (i) that the data user intends to so provide the personal data; and (ii) that the data user may not so provide the data unless the data user has received the data subject's written consent to the intended provision; (b) provide the data subject with the following written information in relation to the intended provision—	Liable on conviction to (if the data is provided for gain) a fine of $1,000,000 and to imprisonment for 5 years; (if the data is provided otherwise than for gain) a fine of $500,000 and to imprisonment for 3 years

Section	Offence	Penalty
	(i) if the data is to be provided for gain, that the data is to be so provided; (ii) the kinds of personal data to be provided; (iii) the classes of persons to which the data is to be provided; and (iv) the classes of marketing subjects in relation to which the data is to be used; and (c) provide the data subject with a channel through which the data subject may, without charge by the data user, communicate the data subject's consent to the intended provision in writing.	
35K (Data user must not provide personal data for use in direct marketing[8] without data subject's consent)	A data user who has complied with section 35J must not provide the data subject's personal data to another person for use by that other person in direct marketing unless— (a) the data user has received the data subject's written consent to the intended provision of personal data, as described in the information provided by the data user under section 35J(2)(b), either generally or selectively; (b) if the data is provided for gain, the intention to so provide was specified in the information under section 35J(2)(b)(i); and (c) the provision is consistent with the data subject's consent. A data user who contravenes the above commits an offence.	Liable on conviction to (i) (if the data user provides the personal data for gain) a fine of $1,000,000 and to imprisonment for 5 years (ii) (if the data user provides the personal data otherwise than for gain) a fine of $500,000 and to imprisonment for 3 years
35L (Data subject may require data user to cease to provide personal data for use in direct marketing[8])	A data subject who has been provided with information by a data user under section 35J(2)(b) may, at any time, require the data user— (a) to cease to provide the data subject's personal data to any other person for use by that other person in direct marketing; and (b) to notify any person to whom the data has been so provided to cease to use the data in direct marketing. A data user who receives a requirement from a data subject must, without charge to the data subject, comply with the requirement. Failure to comply with the requirement is an offence.	Liable on conviction to (if the contravention involves a provision of personal data of a data subject for gain) a fine of $1,000,000 and to imprisonment for 5 years; or (in any other case) a fine of $500,000 and to imprisonment for 3 years.

[8] "Direct marketing" means
(a) the offering, or advertising of the availability, of goods, facilities or services; or
(b) the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes,
through direct marketing means

Section	Offence	Penalty
	If a data user is required to notify a person to cease to use a data subject's personal data in direct marketing under a requirement referred to in section 35L(1)(b), the data user must so notify the person in writing. A person who receives such a written notification from a data user must cease to use the personal data in direct marketing in accordance with the notification. The person who contravenes the above commits an offence.	Liable on conviction to a fine of $500,000 and to imprisonment for 3 years
50A (Offences relating to enforcement notices)	Contravenes an enforcement notice on a first conviction	A fine at level 5 ($25,001 to $50,000) and imprisonment for 2 years If the offence continues after the conviction, to a daily penalty of $1,000
	Contravenes an enforcement notice on a second or subsequent conviction	(A fine at level 6 ($50,001 to $100,000) and imprisonment of 2 years If the offence continues after the conviction, to a daily penalty of $2,000
	A data user who, having complied with an enforcement notice, intentionally does the same act or makes the same omission in contravention of the requirement under this Ordinance, as specified in the enforcement notice	Liable on conviction to a fine at level 5 ($25,001 to $50,000) and imprisonment of 2 years If the offence continues after the conviction, to a daily penalty of $1,000

Section	Offence	Penalty
50B (Offences relating to failure to comply with requirements of [Privacy] Commissioner etc)	(a) Without lawful excuse, obstruct, hinders or resists the Commissioner or a prescribed officer in performing the functions or exercising the power of the Commissioner or the officer; (b) Without lawful excuse, fails to comply with any lawful requirement of the Commissioner or a prescribed officer; or (c) In the course of the performance or exercise by the [Privacy] Commissioner or a prescribed officer of functions or powers under this Part— (i) makes to the Commissioner or the officer a statement which the person knows to be false or does not believe to be true; or (ii) otherwise knowingly misleads the [Privacy] Commissioner or the officer.	Liable on conviction to a fine at level 3 ($5,001 to $10,000) and imprisonment for 6 months
63B (Due diligence exercise)	If a data user transfers or discloses personal data to a person for the purpose of a due diligence exercise to be conducted in connection with a proposed business transaction, the person— (a) must only use the data for that purpose; and (b) must, as soon as practicable after the completion of the due diligence exercise— (i) return the personal data to the data user; and (ii) destroy any record of the personal data that is kept by the person. A person who contravenes the above commits an offence.	Liable on conviction to a ine at level 5 ($25,001 to $50,000) and imprisonment for 2 years
64 (Offences for disclosing personal data obtained without consent from data users)	A person commits an offence if the person discloses any personal data of a data subject which was obtained from a data user without the data user's consent, with an intent (a) to obtain gain in money or other property, whether for the benefit of the person or another person; or (b) to cause loss in money or other property to the data subject.	Liable on conviction to a fine of $1,000,000 and imprisonment for 5 years.
	A person commits an offence if (a) the person discloses any personal data of a data subject which was obtained from a data user without the data user's consent; and (b) the disclosure causes psychological harm to the data subject.	Liable on conviction to a fine of $1,000,000 and imprisonment for 5 years.
64A (Miscellaneous offences)	Without reasonable excuse, contravenes any other requirement under this Ordinance other than those provisions listed in section 64A(2)	Liable on conviction to a fine at level 3 ($5,001 to $10,000)

Annex 3

Relevant offences in existing laws

Existing offences that may involve access, use, retention, etc of data or information contained in a computer

Telecommunication Ordinance (Cap. 106)		
Section	**Offence**	**Penalty**
27A (Unauthorized access to computer by telecommunications)	By telecommunications, knowingly causes a computer to perform any function to obtain unauthorized access to any program or data held in a computer	Liable on conviction to a fine at level 4 ($10,001 to $25,000)

Crimes Ordinance (Cap. 200)		
Section	**Offence**	**Penalty**
60 (Destroying or damaging property)	Without lawful excuse destroys or damages any property[9] belonging to another intending to destroy or damage any such property or being reckless as to whether any such property would be destroyed or damaged Without lawful excuse destroys or damages any property[9], whether belonging to himself or another- (a) intending to destroy or damage any property or being reckless as to whether any property would be destroyed or damaged; and (b) intending by the destruction or damage to endanger the life of another or being reckless as to whether the life of another would be thereby endangered	Liable on conviction upon indictment to imprisonment for life

[9] "Property" means, among others, any program, or data, held in a computer or in a computer storage medium, whether or not the program or data is property of a tangible nature.
"To destroy or damage any property" in relation to a computer includes the "misuse of a computer", which means-
(a) to cause a computer to function other than as it has been established to function by or on behalf of its owner, notwithstanding that the misuse may not impair the operation of the computer or a program held in the computer or the reliability of data held in the computer;
(b) to alter or erase any program or data held in a computer or in a computer storage medium;
(c) to add any program or data to the contents of a computer or of a computer storage medium,
and any act which contributes towards causing the misuse of a kind referred to in paragraph (a), (b) or (c) shall be regarded as causing it.

Crimes Ordinance (Cap. 200)		
Section	**Offence**	**Penalty**
71 (The offence of forgery)	makes a false instrument, with the intention that he or another shall use it to induce somebody to accept it as genuine, and by reason of so accepting it to do or not to do some act to his own or any other person's prejudice	Liable on conviction on indictment to imprisonment for 14 years
161 (Access to computer with criminal or dishonest intent)	Obtains access to a computer- (a) with intent to commit an offence; (b) with a dishonest intent to deceive; (c) with a view to dishonest gain[10] for himself or another; or (d) with a dishonest intent to cause loss[10] to another whether on the same occasion as he obtains such access or on any future occasion	Liable on conviction upon indictment to imprisonment for 5 years

[10] "gain" (獲益) and "loss" (損失) are to be construed as extending not only to gain or loss in money or other property, but as extending to any such gain or loss whether temporary or permanent; and-
(a) "gain" (獲益) includes a gain by keeping what one has, as well as a gain by getting what one has not; and
(b) "loss" (損失) includes a loss by not getting what one might get, as well as a loss by parting with what one has.