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
(Issues of concerns raised by the Privacy Commissioner for Personal Data)

This paper sets out the Administration's response to the issues of concerns raised by the Privacy Commissioner for Personal Data (PCPD) and other deputations in respect of privacy protection in the Electronic Health Record Sharing System (eHRSS).

General Comments

2. We note that the majority of the deputations including PCPD support the enactment of an electronic health record (eHR)-specific legislation. Many of them have indicated that they are looking forward to the early commencement of operation of the Stage One system which includes the basic functions and features of sharing, to be followed by the continual development of the Stage Two system with enhanced functionalities. We also note that many are interested in further collaboration with the Government in new promotional or technical development initiatives.

PCPD's Concerns

3. PCPD has raised a number of concerns regarding the eHRSS Bill in his written submission to the Bills Committee as well as at the meeting on 26 May 2014. Our responses are set out below:

(i) eHR-specific legislation's compatibility with the Personal Data (Privacy) Ordinance ("Privacy Ordinance")

4. In formulating the legislative framework of the eHRSS, the Administration has sought the advice and input of the Steering Committee

on eHR Sharing (EHRSC)[1] and its Working Group on Legal, Privacy and Security (WGLPS). Their membership includes representatives of healthcare professional bodies, patient groups, relevant government departments and statutory bodies. The representatives of PCPD have actively participated in the WGLPS discussion and the majority of their suggestions have been accepted. In essence, we share the view that the privacy protection offered to the healthcare recipients (HCRs)' personal data collected, maintained and used in the eHRSS would not be less than those provided under the Privacy Ordinance. We agree that the personal data contained in the eHRSS would be subject to the regulation of the Privacy Ordinance. PCPD, as the overarching regulator on personal data, would have oversight over the use of personal data contained in the eHRSS. As regards the several areas where arrangements different from the usual Privacy Ordinance practices are considered necessary, the rationale will be explained below.

(ii) Sharable scope of data

5. Most healthcare providers (HCPs) will continue to maintain their own medical record systems after the launch of the eHRSS. Not all the health information contained in the medical records kept by HCPs will be uploaded and shared under the eHRSS. The design of the Stage One eHRSS is to only capture those essential data within a pre-defined scope for sharing. We have set out in the public consultation document the scope of data for sharing in Stage One eHRSS:

- Personal identification and demographic data
- Adverse reactions and allergies
- Summary of episodes and encounters with HCPs
- Diagnosis, procedures and medication

[1] The EHRSC, chaired by the Permanent Secretary for Food and Health (Health), has been providing advice and steer on the development of the eHRSS since 2007. Representatives of key stakeholders in the public and private sectors (including the Hospital Authority, the Office of the PCPD, patient groups, healthcare-related professional bodies, and the Office of the Government Chief Information Officer) have been engaged in the EHRSC and its Working Groups. We intend to retain the same advisory structure upon commencement of operation of eHRSS.

- Laboratory and radiology results
- Other investigation results
- Clinical note summary
- Birth and immunization records
- Referral between providers

6. In drawing up the sharable scope of data, we need to not just identify and define the types of health data, but also determine the formats and standards of such data. The process requires expert advice from the clinical need perspective. Since the inception of the eHR programme, we have been working with professionals in defining the scope. We have been mindful not to collect or share excessively. We have established and consulted expert domain groups, working groups and the EHRSC before finalising the scope for Stage One sharing. These groups comprise healthcare professionals, representatives of patients groups, IT experts, specialists in particular streams (e.g. Hong Kong Academy of Medicine, Hong Kong College of Pathologists, Hong Kong College of Radiologists, Hong Kong Society of Medical Informatics) and standards bodies (e.g. GS1, HL7 Hong Kong). Reference has also been made to the sharable scope of data used in the pilot Public Private Interface-Electronic Patient Record (PPI-ePR) project[2]. Based on the findings of two large-scale patient surveys, we are satisfied that the scope in the pilot was acceptable to the public and not excessive. During our public consultation in late 2011 to early 2012, no adverse comment on the proposed sharable scope was received.

7. The determination of the Stage One sharable scope of eHRSS has gone through a long and thorough discussion and consultation process under a stringent governance structure. Any future amendment to the scope will need to go through the same process under similar governance structure. Meanwhile, patients will be informed about the sharable

[2] PPI-ePR was a pilot project to test the concept of eHR sharing, which started in 2006, for healthcare professionals working in the private sector to access a defined scope of patients' data from the Hospital Authority's electronic patient records.

scope before they decide whether to join the eHRSS via websites[3], "patient information notice" and various publicity materials.

(iii) The "need-to-know" principle

8. PCPD advocates that the "need-to-know" principle should be incorporated in the eHRSS Bill. We wish to clarify that the "need-to-know" principle has been adopted in the design of the eHRSS, and reflected in the relevant legislative provisions and operation/workflows.

9. The "need-to-know" principle is not a new concept that only applies to the data and information in the eHRSS. To ensure the health data in the eHRSS would not be used by or accessible to those without the "need to know", we have incorporated this concept in drafting the clauses relating to the use of data and information contained in the eHRSS. In this regard, Part 3 of the Bill sets out the restriction on the "use" of data and information in the eHRSS. In particular, clause 25 includes a *general prohibition* of use of data and information contained in an eHR. Clause 26 provides that the data and information of a registered HCR may be used for improving the efficiency, quality, continuity or integration of the healthcare provided (or to be provided) to the HCR. This would guard against the use of data and information by any person who has nothing to do with improving the efficiency, quality, continuity or integration of the healthcare provided to the HCR (In other words, those without the need to provide healthcare to the HCR would not be allowed to use the eHR under clause 26).

10. Apart from Part 3, we wish to point out that clause 12 of the Bill setting out the mechanism for the giving of sharing consent to individual HCPs also reflects the "need-to-know" principle. Through this sharing consent, an HCR has the choice over granting access only to those HCP(s) that has (have) a need to know his/her health data in the eHRSS. The

[3] The scope is currently available at the website of the eHR Office of the Food and Health Bureau. It will be available at the future website of the office of the Commissioner for Electronic Health Record (eHRC).

HCR can also revoke the sharing consent given to a particular HCP at any time should he consider that the HCP has no need to access his eHR anymore.

11. The existing Data Protection Principles (DPPs) of the Privacy Ordinance will remain applicable to the personal data in the eHRSS after it commences operation. Although the Privacy Ordinance also does not have a specific definition on "need-to-know", we note that the concept is also embodied in the DPPs. For example, according to DPP3, a data user shall not use the personal data of a data subject for a purpose which is different from or is not directly related to the purposes for which such personal data was collected, unless the data subject has agreed to the "new purpose". In the light of DPP3, the need of any individual in a HCP to know a HCR's data in the eHRSS must be restricted to the purpose of "improving the efficiency, quality, continuity or integration of the healthcare" as stated in clause 26 of the Bill (unless the HCR has agreed to any "new" use).

12. According to DPP4, all practicable steps shall be taken to ensure that personal data held by a data user are protected against unauthorized or accidental access, processing, erasure, loss or use. It follows that in the light of DPP4, an HCP has to make sure that only the relevant individuals in the HCP can access the data and information contained in the eHR for the purpose of "improving the efficiency, quality, continuity or integration of the healthcare" as stated in clause 26 of the Bill.

13. Apart from the legislative provisions, we have also designed the future operation/workflows of the eHRSS in such a way to incorporate the "need-to-know" principle. Like many other major computer systems, the eHRSS will have access control features built in the system. As explained in the public consultation document on the "Legal, Privacy and Security Framework for eHR Sharing", access to the health data in eHR by healthcare professionals would only be granted to those who have valid registration status contained in the statutory professional registers. Administrative staff in an HCP who has a role in the handling of registration or sharing consent of an HCR will only be given access to the

HCR's index data (such as name, address, mobile phone number). All accesses will be logged and traceable.

14. Another important system alert feature is that the access of an HCR's eHR will trigger the issue of a notification (such as SMS) to the relevant HCR. All the above legislative, operational and system designs would work together to ensure that the health data of an HCR would only be accessed by the relevant healthcare professional who has the "need to know" the information when providing healthcare to the HCR.

(iv) "Safe deposit box" feature

15. Conceptually, "safe deposit box" is an electronic data feature which would allow the separate storage of certain patient data with enhanced access control. In the context of eHR, this would mean allowing patients to prevent some categories of eHR sharable data from being automatically viewable by HCPs even with prior general consent obtained from the patients.

16. We recognise that some patients are particularly concerned about the sensitivity of some of their health data and would urge for provision of extra access control. On the other hand, we see the need to balance extra protection for such sensitive data against the completeness and integrity of the eHR to ensure the quality of healthcare delivery. In our response to the issues raised by members at the meeting on 19 May 2014 (LC Paper No. CB(2)1580/13-14(07)) we have set out the pros and cons of providing the "safe deposit box" feature, explained how the current design of the eHRSS provides the flexibility for patients to control access to their health data, and highlighted that the bill, as currently drafted, does not preclude the provision of such feature in future.

17. The Finance Committee (FC) of the Legislative Council (LegCo) approved $702 million for implementing the 5-year Stage One eHR Programme in 2009 (vide LC Paper No. FCR(2009-10)37). As set out in the FC paper, our Stage One target is to develop the basic core infrastructure by 2014 to enable eHR sharing. The "safe deposit box"

was not included as an item in the scope of Stage One eHRSS. Subsequently, during the two-month public consultation in December 2011 to February 2012, the issue of whether any "safe deposit box" should be developed was raised for discussion. There were then divergent views received on the issue. Some patients expressed preference for enhancing protection of certain more sensitive health data. Yet, there were also views expressing concerns over the implications on quality of healthcare delivery, patient safety, risk to healthcare professionals, and practical difficulties for patients to determine which particular data should be regarded as "sensitive". Given the divergent views, when we reported the outcome of the consultation to the LegCo Panel on Health Services in June 2012, we undertook to conduct further study on additional access control over sensitive data during Stage Two with reference to overseas experiences.

18. At the meeting of the Bills Committee with deputations on 26 May 2014, we noted that similar to the last public consultation, there were divergent views on the issue of safe deposit box as summarized below (order of deputations arranged by speaking order):

Views – number of deputations in brackets	**Name of deputations**
Supported the "safe deposit box" concept:	
(a) expressly asked for inclusion of the "safe deposit box" in Stage One of eHRSS Programme (1)	Civic Party
(b) no explicit request on the timing of the provision (4)	Professor John Bacon-Shone, Office of the Privacy Commissioner for Personal Data, Mr Ng Kwok-keung, Dr. Winnie Tang Shuk-ming

(c) supported the concept but accepted that if the "safe deposit box" could not be provided in Stage One, then the Administration should undertake to address the issue properly at the next stage (2)	Hong Kong Alliance of Patients' Organizations Limited, System Aid Medical Services Limited
Expressed reservation / doubts about viability / objection (7)	Senior Citizen Home Safety Association, Alliance for Renal Patients Mutual Help Association, The Association of Licentiates of Medical Council of Hong Kong, Hong Kong Medical Association, Dr Ashley Cheng Chi-kin, Hong Kong Dental Association, Hong Kong Academy of Medicine
No strong inclination on the "safe deposit box" issue but suggested more time to explore the IT solutions / early launching of Stage One system. (8)	Ms June Lui Wing-mui, Hong Kong Computer Society, Sin-Hua Herbalists' & Herb Dealers' Promotion Society Limited, Hong Kong Registered Chinese Medicine Practitioners Association, Mobigator Technology Group, Hong Kong Private Hospitals Association, Hong Kong Society of Medical Informatics, eHealth Consortium Limited

19. The eHRSS is an important infrastructure for use by HCPs to provide better healthcare services to patients. Support and participation of both the healthcare sector and patients are of utmost importance to

ensure successful operation of the new system. Different concerns of the major stakeholders could not be ignored and we need to prudently strike a balance between patients' privacy and patients' safety.

20. Pending a further in-depth study, our preliminary research on overseas experience shows that there are various approaches for offering such functional feature, with different relative emphasis between patients' privacy and patients' safety as well as different implications on system design and clinical workflow. However, most face various problems such as those mentioned above and concerns / reservations from stakeholders particularly HCPs. None of the overseas experiences is particularly successful to date. In a study report published by the World Health Organization (WHO) in 2012 on the legal framework for electronic health in over 113 responding countries, it was found that most countries (85%) did not implement options for patients to conceal or delete information in their eHR. Countries are in general concerned about the negative impact on the quality of care provided and the liability issue arising from management decisions based on incomplete health record. As also pointed out in the WHO report, success of eHR shall be based on trust between patients and their healthcare professionals. An outline of several countries' experiences is set out in the ensuing paragraphs:

Australia

21. The Australian Medical Association has recently criticized the Australian Personally Controlled Electronic Health Record System (PCEHR) that "the ability of patients to remove or restrict access to information in the PCEHR undermined its usefulness, because doctors could not be confident that it provided the comprehensive medical information needed to make an accurate diagnosis or properly assess the safety of proposed avenues of treatment". Meanwhile, the Australian Dental Association stated that "to achieve optimal and effective health care outcomes requires collaboration between patients and health care providers. As currently designed, the control by patients as to the type of information that can be shared with clinicians fails to recognize the

risk this creates to patient safety".

22. A review of PCEHR by a panel of health and IT experts engaged by the Australian Government in end-2013 came up with 14 common concerns and 38 corresponding recommendations. Of relevance to the "safe deposit box" feature was a recommendation to implement a minimum composite of records, which must initially include demographics, current medications and adverse events, discharge summaries and clinical measurements. It was also suggested that the ability for patients to block access to, or remove, certain parts of their record should be reconsidered.

United Kingdom

23. The National Health Service of the United Kingdom undertook a consultancy study to assess the risk to patient safety versus risk to confidentiality in respect of three options ("sealed envelope" (where confidential information is held in the sharing platform), "alternative sealed envelope" (where confidential information is held locally) and "without sealing") in the eHR. Patient safety risks were found to be higher with sealing than without sealing. A major patient safety risk was related to the sealing of medication during one care episode with medication being provided in a subsequent care episode without knowledge of the medication from previous treatments. Another risk was where the patient's allergy information had been sealed in respect of a previous clinical episode, resulting in a future treatment which brings on a similar allergic reaction. The results shaped and limited the provision of "sealing" feature subsequently, including not to allow sealing of certain essential information e.g. medications and allergy.

24. Meanwhile, it was reported that representatives at the British Medical Association's annual meeting backed a motion which claimed that allowing patients to keep some medical information confidential from other doctors "may lead to significant patient safety concerns and potential harm to patients".

Canada

25. Canada ran into a problem of complicated administrative procedures to allow patients to "mask" and "unmask" a piece of health information in their records. Clinicians are required to discuss thoroughly with the patients the clinical risks and medico-legal liabilities that such actions might bring about before any masking can be applied. General acceptance by healthcare professions and the uptake rates are low.

France

26. The Personal Health Record (Dossier Médical Personnel, DMP) in France was implemented since 2004. The approach there is to make the existence of sealed record invisible to any healthcare professionals (known as *masquage du masquage*, meaning "hiding the hiding") so as not to stigmatize anyone with hidden information. This has created a lot of anxiety among healthcare professionals. Many of them are reluctant to use eHRs as they feel they are not accessible to necessary information they may need in order to best treat a patient. The DMP is still experimental although originally its generalization was scheduled for 2007. In December 2013, only 500,000 records were opened, compared to 5,000,000 contractually hoped for, and very few were really operational.

27. The above are based on preliminary desktop research. Given the complexity of the subject, we therefore consider it necessary to conduct an in-depth study, making reference to overseas experience. The findings will help us decide whether to implement a "safe deposit box" and if so, what the best implementing approach is so as to address the concerns of various stakeholders. We aim to commence the study in the first year of Stage Two of the eHRSS Programme.

28. The draft bill and the present design of the eHRSS have built in control measures to provide security and privacy protection to HCRs. Participation in eHRSS is voluntary and HCRs may choose to give

sharing consent to particular HCP that he/she considers appropriate. HCRs may also revoke any sharing consent given to a particular HCP. The Administration will welcome suggestion for improvement of safeguards for implementation in Stage Two.

(v) Registration as an HCP

29. Clause 17(5)(g) of the bill allows the registration as an HCP by a specified entity that, in the opinion of the Commissioner for the eHR (eHRC), *directly or indirectly provides healthcare* to any HCR. Clause 20 provides that eHRC may register a government bureau or department that "*involves providing healthcare*". PCPD is concerned that the arrangement may be too loose which would in effect widen the sharing of the HCR's eHR.

30. Clause 17(5)(g) is intended to be a provision to deal with applications of registration of HCPs requiring special consideration. In cases where a special entity provides healthcare but falls outside the description of clause 17(5)(a) – (h), then clause 17(5)(g) would provide a last-resort channel for eHRC to register such entity as HCP. Since any entities registered as HCPs would need to separately obtain HCR's sharing consents before they can access and share the HCR's eHR, this would unlikely widen the sharing of HCR's eHR. Nevertheless, if Members generally consider that the clause seems unnecessary, the Administration is prepared to remove it.

31. As for clause 20, it is mainly to cater for Government departments such as the Immigration Department or Correctional Services Department, which would also provide healthcare to detainees. They may find access to eHRSS useful.

(vi) Allowing a person authorized in writing by the data subject to make a data access request (DAR) or data correction request (DCR) on behalf of the data subject

32. Pursuant to Section 17A of the Privacy Ordinance, a person

"authorized in writing" by the data subject could make a DAR or DCR on behalf of the data subject. At present, most organisations including the Hospital Authority are following this standard practice.

33. In the context of the eHRSS, we consider that we should impose stricter control than the Privacy Ordinance over the access of eHR by third parties. This is in regard to concerns over possible abuse of such "authorized in writing" arrangement by dishonest employers or insurers. Clause 38 of the eHRSS bill therefore in effect prohibits such arrangement. We note that some members have also recently expressed similar concerns about unintended or coerced authorization. Nevertheless, the Administration is open to views as to whether clause 38 should be retained or removed.

(vii) Offenses

Unauthorized access by non-computer means

34. eHRSS is an IT system, to which access is mainly through computers. In order to deter unauthorized access via computers, we propose in clause 41(1) to make it an offence if a person knowingly causes a computer to perform a function so as to obtain unauthorized access to data or information contained in an electronic record.

35. The PCPD quoted an example of a doctor forgetting to log out from the eHRSS and a third party gaining unauthorized access to eHR by looking at the screen, and considered that such act might not be caught by the several new offences currently proposed in the bill. Our stance is that criminalizing a particular act is a serious matter which must be justified with compelling reasons. To criminalize the mere act of "unauthorized access" (reading eHR from the screen due to the act of somebody forgetting to log out) not followed by any malicious act (e.g. selling it for direct marketing, disclosing it for gain or causing harm to the data subject) could arguably be disproportionate. Unauthorized access to an eHR alone (such as the aforementioned example) is not a premeditated act. In fact, even under the current privacy protection

regime in the Privacy Ordinance, the mere act of accessing one's personal data without consent is also not an offence.

36. The eHRSS bill is intended to provide for the establishment and operation of the eHRSS and the protection of relevant data and information. We consider that data not directly obtained from the eHRSS should not be governed by any offence provision under this bill. If the public is of the view that unauthorized access of personal data without subsequent malicious act in general should be criminalized, the PCPD may wish to consider amending the Privacy Ordinance accordingly in the light of the across-the-broad implications. Once the Privacy Ordinance is amended to reflect the new arrangement, we would review the future eHRSS Ordinance accordingly.

"Misuse" of eHR in general

37. The PCPD has proposed that "misuse" of data for purposes unrelated to the healthcare of the HCR should be made offences. However, we also consider that the term "misuse" carries a broad meaning. There are different extents and various scenarios of "misuse" and it is debatable whether all "misuses" should result in criminal liability. From the law enforcement or prosecution perspective, it may not be appropriate to create an offence to cover generally all "misuses of eHR data".

38. At present, "misuse" of personal data is governed by DPP3 of the Privacy Ordinance. As the PCPD explained in his submission, breaching of DPP3 is not an offence, but the PCPD could issue enforcement notice to the data user and non-compliance of enforcement notice is an offence. We understand that there was a proposal to make contravention of a DPP an offence in the review of the Privacy Ordinance in 2011, which was not pursued given that the majority view in public consultation was against it. Most of the opponents then were concerned with the significant impact on civil liberties, the heavy burden on data users, and the impact on flexibility of DPPs as high-level guiding principles, among others. As this is a wider issue concerning the power

of the PCPD in general, we would defer to the PCPD to separately raise it again for consultation with the public and the Administration.

(viii) Inspection of local Electronic Medical Record (eMR) systems of HCPs

39. Local eMR systems of HCPs are systems used by individual HCP for their own operational and clinical needs. These local eMR systems are **NOT** part of the eHRSS and are thus outside the ambit of the eHRC. Depending on the different operations of HCPs, their local eMR systems may contain other information not related to eHRSS, e.g. personal information of those patients **not** participating in the eHRSS, staff performance of HCPs, and business / financial data of HCPs, etc. In general, only part of the data in HCPs' local eMR systems will be shared under the eHRSS (i.e. only those health data within the defined sharable scope in relation to an HCR who has joined eHRSS and has given a sharing consent to the relevant HCP will be shared).

40. The eHRC, as the system operator and administrator of the eHRSS, is regarded as a "data user" in the context of the Privacy Ordinance. The Privacy Ordinance would be applicable in general to the personal data in the eHR. Accordingly, the eHRC will strive to ensure that the use of eHRSS would comply with the requirements under the Privacy Ordinance For example, in line with DPP4 of the Privacy Ordinance, the eHRC will take practical steps to ensure safe connection to our eHRSS. We have adopted the concept of "building security in" in the development of eHRSS. There are technical measures and controls (such as user/system authentication, access logging and encryption) to ensure safe connection of local eMR systems of HCPs with the eHRSS. Additionally, relevant HCPs must register with the eHRC in prior and satisfy the security compliance requirement before they connect to the eHRSS. Prescribed HCPs could only connect to eHRSS through designated connection modes (such as dedicated leased lines connection, virtual private networks, pre-registered fixed IP address or eHRSS-provided security module).

41. Separately, the eHRC already has sufficient means under the eHRSS Bill to require HCPs to ensure security of their local eMR systems. Examples include clause 18(2) (stipulating that the eHRC could specify the requirements for connecting HCP to the eHRSS, and system requirements on data sharing, for registration as HCPs) and clause 35 (stipulating the requirement that a prescribed HCP must take reasonable steps to ensure that its local eMR system does not impair the security or compromise the integrity of the eHRSS). This is similar to the case of inter-bank clearing system[4]. The eHRC will also monitor the security compliance of local eMR systems through periodic security assessment submitted by HCPs.

42. Individual HCPs, who are the owner and user of their eMR system, are "data users" in respect of their own eMR in the context of the Privacy Ordinance. Accordingly, individual HCPs will need to ensure that the use of their eMR complies with the Privacy Ordinance. The powers of the PCPD over these HCPs are unaffected by the eHRSS Bill (e.g. powers to investigate, inspect, issue enforcement notice, etc).

43. Ensuring the content accuracy of data entered into local eMR systems of HCPs for uploading to the eHRSS is the responsibility of HCPs, as required under DPP2 of the Privacy Ordinance, the Code of Professional Conduct promulgated by the Hong Kong Medical Council and the Code of Practices promulgated by various regulatory Professional Boards and Councils in Hong Kong. However, the data in the eHRSS are mainly medical data of the patients, which are largely professional assessment / opinion of healthcare professionals. They were contributed by the HCPs, not the eHRC. The eHRC, as the system administrator, has no authority to vet nor the expertise and historical knowledge to check the content accuracy of such data. That said, when the health data is shared to the eHRSS, the eHRC will take reasonably practicable steps to ensure the validity of data such as usage of standardized codes and correct matching of person master index data with the health data.

[4] The inter-bank clearing system is a central system that accepts transactions from various banks. The bank's local system would not be regarded as part of the interbank clearing system, although the bank would need to comply with the interfacing protocols imposed by the central clearing system.

44. Inspection of local eMR systems of HCPs, which are not part of the eHRSS and may contain a lot of other sensitive information not relevant to eHR sharing, is highly intrusive. Granting the eHRC with the power to do so is disproportionate to the need and will deter HCPs from joining the eHRSS.

45. As it is not reasonably practicable for the eHRC to inspect or commit to inspect local eMR systems of HCPs, clause 57(2) of the Bill stipulates that the eHRC is not obliged to inspect, or commit to inspect, an eMR system to ascertain—

(a) whether the ordinance is complied with; or
(b) whether any sharable data provided to the eHRSS is accurate.

The implication of this clause is that where a claim is brought against the Government on the ground that the Government has not inspected the eMR systems to ascertain (a) or (b), the claim should fail for lack of merits. It is intended for preventing possible unmeritorious litigations against the Government. Similar clauses can be found in a number of ordinances concerning land, buildings and infrastructure[5].

Food and Health Bureau
10 June 2014

[5] The Buildings Ordinance (Cap. 123), the Eastern Harbour Crossing Ordinance (Cap. 215), the Tate's Cairn Tunnel Ordinance (Cap. 393), the Western Harbour Crossing Ordinance (Cap. 436), the Land Drainage Ordinance (Cap. 446), the Land Survey Ordinance (Cap. 473), and the Tai Lam Tunnel and Yuen Long Approach Road Ordinance (Cap. 474).