OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
— for —
British Columbia

October 5, 2001

Investigation Into BC Nurses' Union Complaint About Telus-VGH LastWord Contract

The attached Investigation Report 01-01 addresses a complaint made by the B.C. Nurses' Union regarding a package of contracts between Telus and Vancouver Hospital and Health Sciences Centre ("Vancouver Hospital"). The complaint focused on concerns about whether the contracts, or procedures under them, comply with Vancouver Hospital's obligations regarding the privacy of patients' personal information under Part 3 of *Freedom of Information and Protection of Privacy Act* ("Act").

The complaint was originally investigated by Sharon Plater, a Portfolio Officer in this Office. It was later taken over by Al Boyd, another Portfolio Officer. I have reviewed Investigation Report 01-01, with emphasis on the findings and recommendations. I agree with the findings and the recommendations respecting contracting-out of services that involve personal information. As the report indicates, I have already made clear my deep concern that all public bodies must ensure that, where they contract-out services or functions, the relevant contracts contain effective, comprehensive provisions relating to privacy and access issues.

I ask Vancouver Hospital to accept the recommendations in Investigation Report 01-01, the implementation of which is necessary, in future, to address Vancouver Hospital's obligations under Part 3 of the Act.

ORIGINAL SIGNED BY

David Loukidelis
Information and Privacy Commissioner
for British Columbia

INVESTIGATION REPORT 01-01

INVESTIGATION INTO A COMPLAINT REGARDING CONTRACTUAL ARRANGEMENTS BETWEEN VANCOUVER HOSPITAL & TELUS

October 5, 2001

Document URL: http://www.oipcbc.org/investigations/01-01.pdf
Office URL: http://www.oipcbc.org
ISSN: 1198-6182

1.0 PURPOSE OF THIS DOCUMENT

[1] This document deals with a complaint to the Information and Privacy Commissioner for British Columbia ("Commissioner") under s. 42 of the *Freedom of Information and Protection of Privacy Act* ("Act") regarding the potential for patient information in the custody or under the control of the Vancouver Hospital and Health Science Centre ("Vancouver Hospital") to be at risk of improper use or disclosure because of a contractual arrangement between the Vancouver Hospital and BC Tel, now Telus. The contract consists of a Master Agreement, Implementation Services Agreement and Services Agreement. (These contracts are referred to in this investigation report, collectively, as the "Contract".)

[2] The package of agreements granted the Vancouver Hospital the right to use the LastWord electronic patient information system and for Telus to provide the Vancouver Hospital with the technical resources to implement and maintain the LastWord system.

[3] This report focuses on the history of the development of the Vancouver Hospital-Telus contract and current understanding of the contract's obligations in light of Vancouver Hospital's obligations, under Part 3 of the Act, regarding the privacy of personal health information in its custody or control. It also offers recommendations in relation to both the current contract and in relation to Vancouver Hospital entering into future contracts involving personal information.

[4] I prepared this investigation report with the assistance of Bill Trott, Portfolio Officer, both of the Office of the Information and Privacy Commissioner ("OIPC").

2.0 BACKGROUND

[5] In April of 1999 the British Columbia Nurses' Union ("BCNU") wrote the then Information and Privacy Commissioner, David Flaherty, and asked that he inquire into

the contractual arrangements surrounding the development of the Vancouver Hospital's then new information system, LastWord. The BCNU was concerned about the implications of some of the language contained in the Contract. Concern was also expressed as to what remedies there might or might not be where a public body, covered by the Act, enters into an agreement with a private agency that is not subject to any privacy legislation.

[6] The BCNU's concerns about the contract language focussed to a large extent on the Master Agreement, section 6.1, and the Services Agreement, clause 5(c).

[7] Section 6.1 of the Master Agreement reads as follows:

> As BC TEL and its subcontractors will have access to information covered by the British Columbia *Freedom of Information and Protection of Privacy Act* (the "FOI and Privacy Act"), it will comply with all of the provisions of that legislation and applicable regulations, and it will require all of its subcontractors to do so, but the Hospital may not terminate this or any other of the PCIS Contracts merely as a consequence of BC TEL or one of its subcontractors failing to comply with the FOI and Privacy Act. The Hospital's Data will be handled by BC TEL in accordance with BC TEL's security procedures as set out in BC TEL's *Security Procedures General Information* document, a copy of which is attached as Exhibit "A". The Hospital agrees that, subject to the FOI and Privacy Act, these procedures, together with the procedures stated below, satisfy the Hospital's current requirements for the protection of the Hospital's Data. Notwithstanding the foregoing, the Hospital reserves the right to extend or alter these procedures based on external legislated requirements. The Hospital may adopt additional procedures for protecting Hospital and patient Data in the future. BC TEL will use reasonable efforts to accommodate such changes to the extent practicable in all the circumstances, provided that no such change will impose a change in operations or negatively impact another customer of BC TEL, nor will any such change exceed the capacity of the PHAMIS Software and the Tandem Software and Tandem Hardware. BC TEL may, without liability to the Hospital, make changes to the attached security procedures which BC TEL determines necessary or desirable for BC TEL Data subject to applicable laws.

[8] The BCNU's concerns regarding s. 6.1 were as follows:

- Although the wording appears to bring Telus under the coverage of the Act, any remedies for a violation would be quite limited.
- The wording could limit Vancouver Hospital's capacity to make changes to current practices to further protect patient information if Telus declined to accommodate the changes.
- Telus could make changes to security procedures in violation of the Act without the Vancouver Hospital having any recourse.

[9] Section 5 of the Services Agreement outlines the "Hospital Responsibilities" and states one such responsibility to be,

> … subject to the FOI and Privacy Act and other laws of general application, provide consent and direction for the release of Hospital's reports and other information by BC TELE to any third party having a legitimate need to receive that information as required in the performance of the service;

[10] The BCNU's concern about this clause was that it contains no definition of what might be considered a "legitimate need" for a third party to access personal information, thus increasing the risk that inappropriate accesses could occur.

[11] The BCNU also expressed two general concerns regarding the Contract overall. These concerns are:

- Reference is made to "Hospital Data" and "data supplied or developed exclusively by the Hospital" with no definition as to what constitutes such information; this could give rise to patient information being considered joint property or the property of Telus.
- The wording relating to subcontractors would allow a Telus subcontractor to further subcontract Vancouver Hospital work without the hospital having control over who might be hired.

3.0 JURISDICTION

[12] The Information and Privacy Commissioner may, under s. 42 "monitor how the Act is administered to ensure that its purposes are achieved, and may … conduct investigations and audits to ensure compliance with any provision of this Act". Section 42(2) allows the Commissioner to investigate a complaint that a public body has not performed its duty under the Act. Section 42 also gives the Commissioner the power to issue an order to require that a duty imposed by the Act be performed.

[13] Part 3 of the Act establishes the minimum requirements concerning a public body's collection, use and disclosure of personal information. Section 30 expressly creates a duty in the following terms:

> The head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

[14] Under the Act, "personal information" means recorded information about an identifiable individual.

[15] The Commissioner has the authority to investigate the concerns raised by the BCNU and to issue any order or recommendations that he deems appropriate to ensure that the Vancouver Hospital meets any duties imposed by the Act. The Commissioner has delegated to me the authority under s. 42 of the Act to investigate complaints.

4.0 PROCESS FOLLOWED

[16] The investigation into this complaint included the following steps:

- Detailed review of the complaint letter;
- Detailed review of the contract, services agreement and the implementation services agreement;
- Meeting with Vancouver Hospital staff;
- Review of the IDX Systems Corporation Website;
- Review of the LastWord background documents;
- Review of response letter received jointly from Telus and the Vancouver Richmond Health Board, the public body of which the Vancouver Hospital is part;
- A review of the relevant legislation;
- A review of documents supplied by Telus including its Business Conduct Guidelines, Privacy Code, Administrative Guidelines concerning safeguarding of information and the confidentiality document that employees must sign.

5.0 ISSUES

[17] The following issues were reviewed during the investigation:

1. Whether s. 6.1 of the Master Agreement adequately meets Vancouver Hospital's s. 30 obligation to protect personal information in:

   (a) addressing the custody and/or control of the personal information;
   (b) limiting the termination of the Contract for failure to comply with the Act;
   (c) allowing Telus to refuse to implement any additional privacy protection procedures that would "impose a change in operations";
   (d) permitting Telus to make changes to Telus' security procedures?

2. Whether s. 5(c) of the Services Agreement adequately meets Vancouver Hospital's s. 30 obligation to protect personal information in relation to access to, or use of, such information by a third party or when a subcontractor further contracts out work?

3. Whether Vancouver Hospital's procedures, as opposed to the terms of the Contract, adequately meet its s. 30 obligations to protect personal information?

6.0 DISCUSSION

[18] **6.1 Statement of Facts** – The following facts were discussed and agreed upon with the staff of the Vancouver Hospital and Health Sciences Centre. Some of the facts were also confirmed in writing in a letter jointly submitted by the Vancouver Hospital and Telus.

Background

[19] In 1996, Vancouver Hospital decided to use LastWord Enterprise Clinical Solution as its electronic patient information system. LastWord is owned by IDX Systems Corporation, which had granted the distribution rights to BC Tel (now Telus) for a number of provinces, including British Columbia. Vancouver Hospital thus purchased the right to use the LastWord from Telus.

[20] At the time, Vancouver Hospital was uncertain as to whether or not it had the technical capacity to develop, set into production and then maintain its planned patient information system. Telus appeared to have this capacity and was interested in using Vancouver Hospital to demonstrate this capacity in hopes of selling LastWord to other medical facilities in western Canada. Vancouver Hospital and Telus entered into a contract under which Telus would sell the use of LastWord system to Vancouver Hospital and provide the technical capacity to develop, set into production and maintain the system. Telus provided a project manager and some staff, all of whom reported to the Chief Technology Officer for Vancouver Hospital.

[21] Vancouver Hospital was to provide direction as to what would be required and Telus would provide the technical knowledge to accomplish this. The arrangement would require Telus employees to have access to some patient data in the LastWord system when the system was first implemented, when assisting with technical problems and when testing the system as changes were made.

[22] Vancouver Hospital Information and Privacy staff appear not to have been consulted about the wording of the Contract nor was a Privacy Impact Assessment completed. It is worth noting at this point that, although the use of a Privacy Impact Assessment ("PIA") was not at the time a well-known mechanism or standard recommended practice, as is the case today, its use has been discussed for some time. For example, PIAs were discussed as far back as in the March-April, 1975 edition of the Harvard Business Review. As well, the OIPC published a PIA related to British Columbia provincial ID cards in September of 1995.

[23] The LastWord system went live in November 1997 and, in 1998, Vancouver Hospital started to take direct responsibility for the further implementation and enhancement of its LastWord system. Telus continued to provide resources to assist in this implementation.

[24] There are no other documents, such as letters of understanding, other than the Master Agreement and attachments, the Services Agreement and attachments and the Implementation Services Agreement, which govern the LastWord relationship between Vancouver Hospital and Telus.

[25] The Contract between Vancouver Hospital and Telus expires in June 2002.

Situation Today at Vancouver Hospital

[26] Vancouver Hospital continues with the ongoing implementation of LastWord as its elective patient information system. The implementation has various stages, including a release environment, development environment, a quality assurance environment, a test environment, training environment and, finally, a production environment. Patient information is only available at the production environment level where the system goes live.

[27] Telus staff continue to assist Vancouver Hospital with implementation of LastWord. The assistance is primarily at the development, quality assurance and test stages. However, Telus staff do access some patient information when required to provide assistance in debugging problems and in implementing fixes to the system. These Telus staff report directly to, and take their directions from, a Vancouver Hospital manager, although they continue to be paid by Telus. Vancouver Hospital is fully involved in the selection of any Telus staff person who will be working at Vancouver Hospital. These staff must also go through the same training procedures and sign the same confidentiality agreement as do Vancouver Hospital staff.

[28] If a Telus staff person violated the confidentiality agreement, that individual would be subject to the same sanctions as a regular Vancouver Hospital employee, up to and including removal from the Vancouver Hospital site. Vancouver Hospital expects that Telus would also dismiss such an individual for such an infraction. Telus would appear to be in agreement with this position, as it is referenced in their joint response letter to the OIPC.

[29] Normally, Telus staff at Vancouver Hospital do not provide trouble-shooting technical support to hospital ward staff. Vancouver Hospital has internal Clinical Support Analysts who provide that support. Telus staff could discuss system requirements with ward staff, but such discussions would not necessarily require that Telus staff have access to any patient information.

[30] Vancouver Hospital has full control over the issuing of user-IDs and passwords to all staff, including Telus staff. It thus has the ability to immediately cancel any access to its system should a violation occur. Vancouver Hospital staff also are responsible for all audit processes, including audits of all staff activity on the system staff including both Vancouver Hospital and Telus employees.

[31] Vancouver Hospital is slowly converting all of the Telus positions to regular Vancouver Hospital positions, with the end goal being that the system will eventually be fully maintained by Vancouver Hospital staff.

Situation Today at Telus

[32] A limited number of Telus staff have access to the LastWord system from Telus offices. Two technical support staff provide technical assistance for the Tandem operating environment. Staff at Telus who maintain the Tandem equipment do not have

access to LastWord. The data sent to Telus for this purpose are technical in nature and system maintenance does not require access to patient information. The Telus staff have restricted user-IDs and passwords that limit their level of access to these data, in order to carry out their job functions.

[33] The information is sent between the two sites through two dedicated lines that are not shared with any other customers.

Audit Capacity

[34] The LastWord system has a built-in audit function that electronically logs when anyone undertakes any activity involving the system. Using this system, Vancouver Hospital system security staff are able to produce audit reports detailing who has accessed the record of any specific patient. Vancouver Hospital system security staff also carry out regular random audits of a sampling of the patient files to identify and investigate apparently inappropriate accesses to records in the system.

[35] An audit is conducted, and a report created, any time a complaint is made by patients that their privacy may have been violated. Such reports are forwarded to the Patient Relations Office for their investigation and resolution. To date, there never has been a complaint received, or an audit report, resulting in a determination that a Telus employee has inappropriately accessed patient personal information.

System Security

[36] Access to the LastWord system is controlled through user-IDs and passwords based on the individual's level of authority and job responsibilities. The Vancouver Hospital assigns and revokes these user-IDs and passwords independent of Telus. User-IDs and passwords can be revoked immediately if required.

[37] All LastWord workstations on the wards have been configured to prevent individuals from downloading patient information on to discs.

[38] The Vancouver Hospital systems are designed to prevent the transferring of patient information by email.

[39] Prior to allowing Vancouver Hospital information to be sent to the Telus site, Vancouver Hospital systems staff did a site visit to ensure that the Telus security met or exceeded the Vancouver Hospital and *Freedom of Information and Protection of Privacy Act* requirements. These requirements were apparently exceeded in their view.

[40] **6.2 Vancouver Hospital's Response to Specific Concerns** – Vancouver Hospital's general position on the particular concerns raised by the BCNU complaint is that the wording of the Contract reflects the fact that both Vancouver Hospital and Telus were entering into a new realm and thus wanted to cover any unforeseen matters that might arise, including situations involving other potential Telus LastWord customers. At the time, Telus was seen as having more technical expertise than did Vancouver Hospital

and thus Telus took the lead in determining what was required. Today, Telus does not have control over, nor access to, the Vancouver Hospital system as might have originally been envisioned.

[41] The following discussion sets out Vancouver Hospital's specific responses to issues raised by the BCNU's complaint.

Inability to Terminate for Privacy Breach

[42] Vancouver Hospital's position is that the wording of s. 6.1 was intended to provide Telus with some assurance that the Contract would not be automatically cancelled if a minor breach of the Act occurred, but that instead the two parties would take steps to prevent another such breach. It also reflects the reality, Vancouver Hospital says, that any abrupt decision to terminate the contract would be extremely disruptive and in the short term could compromise patient care.

[43] Vancouver Hospital also takes the position that, regardless of the wording of s. 6.1, any serious or intentional disclosure of personal information by Telus staff would be considered a material breach of the Contract and it would take various steps to remedy the breach, up to and including termination of the Contract.

Telus' Ability to Resist Security Changes

[44] Vancouver Hospital noted that s. 6.1 was written in light of the situation at the time. Telus was planning to market LastWord to other medical facilities, some of which potentially could have been on the same platform as Vancouver Hospital. The clause was intended to allow Vancouver Hospital to make whatever changes it deemed necessary to protect its data, while not requiring the same changes to be made to other customers' systems. Telus would thus have made the changes to meet Vancouver Hospital requirements, but would not have been required to do so for other customers. Vancouver Hospital also noted that no other customers share the Vancouver Hospital platform, so this has never been an issue.

Telus' Ability to Change Security

[45] Vancouver Hospital interprets the intent of s. 6.1 to be to allow Telus to make changes to its security procedures if doing so would enhance its system security. This would typically be a result of a change in industry standards or legislation. It is Vancouver Hospital's belief that Telus is one of the leaders in system security and would want to make changes in order to continue in this leadership role.

[46] The Vancouver Hospital also takes the position that, if any such changes appeared to lessen the security of Vancouver Hospital information systems and Telus insisted on implementing such changes, Vancouver Hospital would consider this a material breach of the Contract.

Patient Information Becoming Property of Telus

[47] Vancouver Hospital's position is that all patient information is the exclusive property of Vancouver Hospital in relation to the Contract. It further notes that, with the exception of Telus personnel supporting the operating environment, Vancouver Hospital is responsible for all desktop equipment, assigns and revokes user rights, and carries out and reports on all audits.

Inappropriate Third-Party Access to Patient Information

[48] Vancouver Hospital apparently cannot foresee a need for any third party to receive patient information, with one possible exception. The only potential third-party access to any Vancouver Hospital patient information would be for the purposes of disaster recovery should the Telus site be incapable of providing services. Early on in the contract, Telus proposed use of a third-party disaster recovery planning service. Telus apparently does a routine back up of its technical data systems and rotates the backup offsite in case of a disaster that causes its site to be inoperable. The backup system can only be used with the Vancouver Hospital system.

[49] Vancouver Hospital notes that patient safety could be compromised if no provision was made for a backup and Telus was unavailable for a long period of time due to a disaster.

Control Over Subcontractors

[50] Vancouver Hospital noted that, because it controls access to patient information, a Telus subcontractor could only access such data with the explicit approval of Vancouver Hospital.

[51] Vancouver Hospital is also of the opinion that it does have control over the hiring of all subcontractors through the Contract's definition of Approved Subcontractors (s. 1.3), through s. 3.3 (which discusses "Approved Subcontractors") and through s. 5(c) of the Service Agreement (which requires Vancouver Hospital consent before its information could be disclosed to a third party). In practice, all such hires over the past 24-36 months have been through a joint Vancouver Hospital-Telus selection process.

[52] **6.3 Discussion of Contract Issues** – The following discussion deals with each of the issues raised by the BCNU complaint. The discussion initially reviews two provisions of the Contract and then discusses the Hospital's procedures.

Do Telus Staff Have Access to "Personal Information"?

[53] It is important to determine whether Telus staff have access to "personal information" in relation to Telus fulfilling its service obligations under the Contract. If Telus does have access to such information, then Vancouver Hospital's legislated responsibilities under s. 30 Act are relevant. If Telus does not have access to personal

information, s. 30 is not a consideration, as it specifically refers to "personal information".

[54] The definition of "personal information" contained in Schedule 1 of the Act reads as follows:

> **"personal information"** means recorded information about an identifiable individual, including
>
> (a) the individual's name, address or telephone number,
>
> (b) the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,
>
> (c) the individual's age, sex, sexual orientation, marital status or family status,
>
> (d) an identifying number, symbol or other particular assigned to the individual,
>
> (e) the individual's fingerprints, blood type or inheritable characteristics,
>
> (f) information about the individual's health care history, including a physical or mental disability,
>
> (g) information about the individual's educational, financial, criminal or employment history,
>
> (h) anyone else's opinions about the individual, and
>
> (i) the individual's personal views or opinions, except if they are about someone else;

[55] Given this definition, if Telus staff have access to patient information through the LastWord system, they have access to personal information. Patient information on LastWord includes name, personal health number, and information relating to admission, diagnosis and treatment. This is all clearly "personal information" under the Act.

[56] Most individuals consider their medical information to be highly sensitive and want its confidentiality protected. When individuals go into a hospital, they place their trust and faith in that hospital to ensure that their privacy is properly protected. Hospitals must take this trust seriously and take whatever steps are required to protect patient information, even if the chances of its being inappropriately disclosed or used are remote. Given this, if Vancouver Hospital believed that there was even a remote chance that Telus staff would have access to patient information, it had a responsibility to ensure that the Contract protected that information from any inappropriate use or disclosure.

[57] Vancouver Hospital has confirmed that some Telus staff do have access to patient information, as outlined in the statement of facts above. Vancouver Hospital thus has a responsibility under s. 30 of the Act to make reasonable security arrangements against risks such as unauthorized access, collection, use, disclosure or disposal of patient information by Telus staff. Both the Contract and Vancouver Hospital procedures must meet the s. 30 test. I will discuss the Contract and then Vancouver Hospital's procedures.

Custody and/or Control of Patient Information

[58] The next issue is the BCNU's concern that the Contract does not clearly stipulate who has ownership of, or control over, patient information that is subject to the Contract. Again, Telus and Vancouver Hospital have said, in relation to this matter, that "all patient information is the exclusive property – and responsibility – of" Vancouver Hospital in relation to the Contract.

[59] The Master Agreement, which is part of the Contract, defines "Data" as all information that is either "used in the performance of Services" under the Contract or that is "resident on or processed by the PCIS" (the patient care information system contemplated by the Contract). Section 6.1 refers to the "hospital's Data" being "handled" by Telus. It also refers, however, to Hospital Data and "patient Data" as if they are separate kinds of data. Section 6.2 requires Telus to protect the confidentiality of "all Data provided by or originating with the Hospital", including "all patient Data". That section goes on to provide that all patient data are "considered private, proprietary and confidential without the need for further designation as such." (It is not clear what is meant by describing patient information as "proprietary", although one might interpret this as meaning that Vancouver Hospital purports to retain ownership of that data.) Last, s. 6.2 provides that all "Hospital Data" continues to be "considered Hospital Data" after processing or reformatting by BC TEL."

[60] In addition, s. 4(h) of the Long-Term Services Agreement requires Telus to follow Vancouver Hospital's instructions for "the disposition of Hospital's Data" once the Contract ends. Section 5 of that contract gives Vancouver Hospital control over use of user-IDs and passwords related to the system, and it also requires Vancouver Hospital to ensure the accuracy and completeness of all data supplied to Telus in connection with the Contract. Further, s. 6 of that contract expressly provides that all data "supplied or developed exclusively" by Vancouver Hospital in the performance of any of the services "remains Hospital's exclusive property".

[61] These provisions, together with other aspects of the Contract (including some of the schedules to the various service agreements) support the position taken by Telus and Vancouver Hospital, *i.e.,* that patient information in the system does not, as a consequence of the Contract, become the property of Telus. As is discussed below, however, the lack of provisions that explicitly address the question of custody or control, and responsibilities under the Act, leaves too much room for interpretation and should be avoided in similar contracts in the future. It should also be noted that the concept of ownership of personal information is not necessarily appropriate in the context of the Act. The Act governs Vancouver Hospital's ability to collect, use, disclose, store and retain personal information about its patients and property-related concepts have little to do with the privacy rights and obligations imposed on Vancouver Hospital by the Act.

Consequences of Failure to Comply with Act

[62] Given that Telus staff do have access to patient information, it is appropriate to review whether the wording of the Contract puts such information at risk of use or disclosure that is not authorized by the Act.

[63] The difficulty in determining the appropriateness of the wording is that much of it is left open to interpretation without the benefit of specific definitions or a section that clearly spells out the intent of the Contract as regards privacy. This could reasonably lead individuals reading the contract to interpret it in a manner other than was intended. This fact is best demonstrated in s. 6.1 of the Contract, which contains three separate clauses that have caused concern for the BCNU.

[64] As is noted above, s. 6.1 of the Contract provides that Vancouver Hospital cannot terminate the Contract "merely as a consequence of BC TEL or one of its subcontractors failing to comply with the FOI and Privacy Act." Both Vancouver Hospital and Telus have, in response to the BCNU's concerns, taken the position that this language, as they put it in their joint letter to the OIPC

> … was intended to provide TELUS with some re-assurance that the contract would not be automatically cancelled if a minor breach of the FOI legislation occurred, but that instead the two parties would take steps to remedy the situation, and prevent another such breach.

[65] Of course, s. 6.1 does not, on its face, say anything of the kind. A reasonable interpretation of the provision, in fact, is that Vancouver Hospital is not entitled to terminate the Contract because of a breach of the Act. The reasonableness of this interpretation is reinforced by the fact that s. 10 of the Contract contains explicit rights of termination, none of which relate to s. 6.1. Either party is entitled, under s. 10, to terminate the Contract only for "a material breach by the other party of a material obligation" under specified provisions of the Contract. Section 10 requires the terminating party to give a considerable period of time for the other party to cure the alleged breach and, in some cases, the parties must first follow a step-by-step correction and resolution procedure, which is specified in ss. 8 and 9 of the Contract. These provisions reinforce the reasonable interpretation of s. 6.1 as precluding termination of the Contract because of a breach of the Act, whether under the explicit termination provisions of s. 10 or any common law right to terminate for fundamental breach. In this light, it is difficult to accept Vancouver Hospital's assertion, at this time, that failure by Telus to address any *intentional* disclosure of personal information by its employees would give Vancouver Hospital the ability to "explore various steps up to remedy [*sic*] the breach up to and including termination of the contract."

[66] The position taken by Vancouver Hospital and Telus in response to the BCNU's complaint about s. 6.1 reveals what both parties say was their intent in agreeing to the language of that section. But because those kinds of assurances are not expressly contained in the Contract, it has to be said that explicit provision for the consequences of

breaching *any* of the Act's requirements should have been contained in the Contract. Since Vancouver Hospital's ability to terminate the Contract is explicitly limited in s. 10, assurances at this time that Vancouver Hospital would attempt, in the face of an *intentional* (but not necessarily negligent) disclosure of patient information, to terminate the Contract seems difficult to reconcile with the express language of s. 10.

Changes to Vancouver Hospital Data Protection Procedures

[67] The second aspect of s. 6.1 that must be addressed relates to the following language in that section:

> The Hospital may adopt additional procedures for protecting Hospital and patient Data in the future. BC TEL will use reasonable efforts to accommodate such changes to the extent practicable in all the circumstances, provided that no such change will impose a change in operations or negatively impact another customer of BC TEL…

[68] In their joint letter to the OIPC, Vancouver Hospital and Telus said that this aspect of s. 6.1 was intended to allow Vancouver Hospital to "make whatever changes it deemed necessary to protect its data, while not requiring the same changes to be made to other customer's systems." While it is true that language of s. 6.1 addresses the possible impact on other Telus customers of any Vancouver Hospital changes in data protection procedures, the section also allows Telus to refuse to implement any additional procedures that would "impose a change in operations". Further, s. 6.1 only requires Telus to "use reasonable efforts to accommodate such changes to the extent practicable in all the circumstances." Although it may have had cost ramifications for Vancouver Hospital, one would hope that a contractor in Telus' position would be *required* to make any such changes that the public body, acting reasonably, considers necessary to meet its obligations under the Act.

Changes to Telus' Security Procedures

[69] The final aspect of s. 6.1 of that is of concern allows Telus to, "without liability to the Hospital", make changes to "Telus' security procedures which BC TEL determines necessary or desirable for BC TEL Data subject to applicable laws."

[70] One could reasonably assume that this clause would allow Telus to lessen its security procedures, rather than enhance them, if it determined that it wished to do so and as long as the changes still met the "applicable laws". Both parties have stated that the intent of this was to allow Telus to make any changes which might be required as a result of a change in industry standards or because Telus determined that it wanted to enhance its security procedures. It was also said that Telus holds a respected position as a leader in systems security and it would not want to do anything that would bring its standing into disrepute. Finally, Vancouver Hospital takes the position that it would consider a change in any security procedures that placed its information systems at risk a material breach of the contract and would act accordingly. (Vancouver Hospital said, "legal measures could well be initiated", but it did not specify how it would act or what legal measures could or would be initiated.)

[71] The above comments about the limited, explicit ability to terminate the Contract under s. 10 also apply here. In the face of the express termination rights under s. 10, it is not clear what other legal recourse Vancouver Hospital would have against Telus for any alleged breach of this kind. Again, it would be better if the Contract expressly spelled out what remedies existed for any change in security procedures by Telus that Vancouver Hospital considered jeopardized its information systems.

Other Third-Party Access to Patient Information

[72] The BCNU expressed the concern that s. 5(c) of the Services Agreement would result in personal information being placed in the hands of third parties. (A third party in this context is a party other than the two parties to the Contract, Vancouver Hospital and Telus.)

[73] Section 5(c) requires Vancouver Hospital, "subject to the FOI and Privacy Act and other laws of general application" to

> … provide consent and direction for the release of Hospital's reports and other information by BC TEL to any third party having a legitimate need to receive that information as required in the performance of the Service.

[74] As was noted above, Telus and Vancouver Hospital say that they cannot "foresee a need for any third party to receive patient information" except in the unlikely event of a disaster such that Telus would not be able to provide services. This does not answer the BCNU's concern, which has to do with whether the Contract adequately addresses the question of third-party access, *i.e.,* prevention of inappropriate third-party access.

[75] In any case, s. 6.2 expressly prohibits BC TEL from disclosing patient information except to " persons authorized by the Hospital to receive such Data" or to personnel of approved subcontractors who have a need to know or use that data in order to perform services and who have signed a confidentiality agreement with Telus. (The question of whether subcontractors should be required to enter into confidentiality agreements directly with Vancouver Hospital, or any other public body in its position in a similar case, is addressed below.)

[76] Disclosure of personal information to contractors, subcontractors and their respective employees is permitted where the disclosed information is necessary for the performance of the duties of the employee (s. 33(f)). Schedule 1 to the Act defines "employee" as including a person retained under a contract to perform services for the public body. The Act, therefore, contemplates disclosure to contractors of personal information on a need-to-know basis in relation to performance of their services for a public body. A public body such as Vancouver Hospital should, however, expressly limit such disclosures, which has been done in s. 6.1 of the Contract.

[77] An example of an appropriate potential third-party disclosure was outlined in the joint letter provided by Vancouver Hospital and Telus. They stated that the *only* potential third-party access would be in the event of a disaster of such magnitude that Telus could

not provide services. Vancouver Hospital also argues that patient safety could be compromised if such arrangements were not made and Telus were unavailable for a considerable length of time. However, the OIPC understands that, in the case of a disaster, only the information needed to run the system would be accessed by the third party. This information is programming information and does not include patient personal information.

Control Over the Hiring of Telus Subcontractors

[78] Another BCNU concern was that the Contract allows for the possibility of Telus' subcontractors further subcontracting out services, which could result in patient information being released.

[79] Section 3.3 of the Master Agreement allows Vancouver Hospital to object to any subcontracting by Telus of services under the Contract. Vancouver Hospital can object, however, only in limited circumstances. If a subcontractor or supplier is a "substantial business entity with a good reputation and established expertise and products", Vancouver Hospital cannot object. In their joint letter to the OIPC, Telus and Vancouver Hospital relied on the fact that subcontractors must, in order to be "Approved Subcontractors", "have reasonable experience and skill." They went on to assert that Telus

> … is not at liberty to subcontract without attention to the principles of confidentiality, nor with agents who do not meet the contractual test of approved sub-contractors.

[80] They did not point to any aspects of the Contract that restrict Telus' "liberty to subcontract", much less in a way that addresses the obligations imposed on Vancouver Hospital under the Act. Nor can much reliance be placed on the assertion that Telus is not free to contract "without attention to the principles of confidentiality", including because "principles of confidentiality" is not sufficient, to import the Act's provisions into the situation.

[81] Although Telus' privacy and confidentiality obligations under s. 6 of the Master Agreement would, implicitly at least, give Telus an incentive to ensure that any subcontract contained similar provisions. It would be preferable (and not unusual these days) for the Contract to expressly require Telus to impose on its subcontractors the privacy aspects of the agreement.

[82] **6.4 Review of Vancouver Hospital's Procedures** – The previous discussion reviewed the provisions of the Contract. Vancouver Hospital argues it has put into place a series of procedures to protect personal information in its custody and/or control from a number of threats, including any unauthorized access, use or disclosure. It says these procedures satisfy its s. 30 obligations.

[83] It has been confirmed that Telus staff do have authorized access to the LastWord patient information system in limited situations. The question thus becomes has the Vancouver Hospital put into place reasonable precautions to ensure that this access does not place patient information at risk.

[84] The access to patient information only occurs onsite at the Vancouver Hospital for the purposes of providing technical assistance in the same manner as do similar Vancouver Hospital staff. The focus on whether the Vancouver Hospital is meeting its s. 30 responsibilities is thus focused on this access. In this regard, the following are considerations.

- All staff are hired via a process that involves Vancouver Hospital, as the Telus staff are hired through a joint selection process involving the Vancouver Hospital
- Both groups go through the same training process and must sign the same Pledge of Confidentiality form
- All staff are directly supervised by and receive their direction from Vancouver Hospital supervisors, including the Telus staff
- These staff work side-by-side at the same locations within the Vancouver Hospital
- The level of system access granted to all staff, including Telus staff, are controlled by the Vancouver Hospital via the issuance of user-IDs and passwords
- System audits would reveal any inappropriate access attempts by Telus staff in the same manner as for the Vancouver Hospital staff
- Telus staff are subject to the same sanctions as Vancouver Hospital staff for any violation of the system security, up to and including dismissal
- Vancouver Hospital has the ability to immediately revoke any staff person's access to the LastWord system, including Telus staff, independent of any Telus involvement
- To date, there have been no complaints about nor audit reports resulting in a determination that a Telus employee has inappropriately accessed the LastWord
- It would appear that on a day-to-day basis, the only difference between these two groups of staff would be that the one group is considered to be Telus employees while the others work directly for Vancouver Hospital

[85] Given the above, it is reasonable to assume that if the Vancouver Hospital's current policies and procedures allow it to meet its s. 30 requirements in relation to its own staff, then the same would be true for the Telus staff who are working along side the Vancouver Hospital staff.

7.0 CONCLUSIONS

[86] **7.1 General Comments About Contract Language** – In their joint letter to the OIPC, Vancouver Hospital and Telus said that their letter set out their "mutual understanding" of the Contract's language with, they acknowledged, "out of context may reasonably appear to be of concern." As the above discussion indicates, it is only with the context provided to the OIPC by Telus and Vancouver Hospital that some of the

apparently problematic Contract provisions have been explained. As a general matter, it is not sufficient for a public body to approach its privacy obligations under the Act in this way when negotiating and settling the terms of a contract of this nature, which involves highly sensitive personal information. At the very least, if Vancouver Hospital's information and privacy staff had been consulted for the purposes of the Contract's negotiation and drafting, one would hope that its provisions would clearly, unambiguously and exhaustively have addressed all of the privacy issues raised by the Contract. In particular, the Contract should have included explicit provisions for the consequences of breaching any of the Act's requirements.

[87] Further, use of a privacy impact assessment tool would have helped to highlight some of the potential concerns and provided answers to some of them in drafting the Contract. Again, the use of PIAs was relatively new at the time the Contract was developed and thus there may not have been an awareness of the availability and usefulness of PIAs.

[88] The next section addresses the specific aspects of the Contract.

[89] **7.2 Custody and/or Control of Patient Information** – It is fairly apparent that the intent of the Contract was to provide for both the right of Vancouver Hospital to use the LastWord product as its patient information system and to contract with Telus to provide the technical services to establish and maintain the system. It would appear that, if Vancouver Hospital had so chosen it could have purchased the LastWord use rights from Telus and made other arrangements to have its technical needs met. Further, as the above discussion indicates, the Contract's terms are reasonably clear as to ownership of the patient information. Ownership is not, again, necessarily the appropriate way of approaching these issues in light of the Act's privacy requirements.

[90] Given the above, I have concluded there was no intent by the parties to create a situation that would see Telus taking ownership of any patient information. In fact, Telus' access to such information has been very limited, to the point of only taking place when required to ensure that new additions to the system are fully operational. Still, such contracts should in future contain much more explicit provisions on this point. They should make it clear the public body retains control of the personal information and remains its custodian. The contract should also clearly define what is personal information and what is not.

[91] **7.3 Does the Contract Adequately Limit Third Party Access?** – Section 5(c) of the Service Agreement in my view provides sufficient protection to ensure that only third parties with sufficient reasons for doing so, and who meet the necessary requirements under the Act, could have access to patient information. This clause should, in my view, be read to mean that the Vancouver Hospital has a responsibility to only consent to the disclosure of patient information to third parties who meet the Act criteria, including s. 33. Having said that, if the intent is that this section is to only allow for third-party access in the event of a disaster, the provision should expressly state this. If there are other legitimate instances of third-party access, they should be clearly spelled out as well.

[92] **7.4 Does the Contract Sufficiently Deal With Use of Subcontractors by a Telus Subcontractor?** – It is my view that the Contract could present concerns due to the potential use of subcontractors by Telus' Approved Subcontractors. Nothing in the Contract was drawn to my attention that would require Telus to require its Approved Subcontractors, through the Telus-Approved Subcontractor subcontract, not to subcontract further or to do so only to similarly "Approved Subcontractors". Since it is not at all inconceivable, in the information systems business, that a Telus subcontractor might seek to subcontract all or part of its tasks, it would have been preferable for the Contract to deal with this.

[93] **7.5 Has Vancouver Hospital Met Its Section 30 Obligations?** –. Based upon the above discussion, I find that the Contract does not adequately address Vancouver Hospital's s. 30 obligations. However, I find that it has sufficient procedures in place to restrict access to patient personal health information and to safeguard it from inappropriate use or disclosure and that these comply with s. 30 of the Act.

[94] It is my view that the Vancouver Hospital has met its responsibility under s. 30 based on the controls it has in place. Telus staff can only access patient information on site at the Vancouver Hospital. The Vancouver Hospital is directly involved in the selection, training, supervision, provision of direction and, if necessary, the disciplining of these staff. Telus staff must sign the same confidentiality statement as do Vancouver Hospital staff. Access to the LastWord system is issued, and can be removed, in the same manner to all staff, including Telus staff, by the Vancouver Hospital.

[95] Again, if the wording in the Contract had made all of this clearer, it would have provided some reassurance to those not involved in the Contract's development that patient information would not be at an increased risk due to the use of Telus staff onsite at Vancouver Hospital.

[96] While the Contract itself does not meet the Hospital's s. 30 obligations, Vancouver Hospital has put into place adequate procedures to meet its s. 30 obligations.

8.0 RECOMMENDATIONS

[97] The following recommendations are directed at Vancouver Hospital in light of the above discussion and after reaching the above conclusions.

1. In relation to the existing Contract, regular audits should be conducted of all Vancouver Hospital and Telus systems staff access to the patient information on the LastWord system for the remainder of the current Contract.

2. Regarding the development of any contracts involving personal information in the future, including any related to the LastWord patient information system, I recommend the following:

   (a) Vancouver Regional Hospital Board ("VRHB") information and privacy staff should be consulted during contract negotiations regarding privacy requirements and related contract wording, including where the contract might involve the use or disclosure of personal information by the contractor or others.

   (b) As part of that consultation, and the business negotiations, a privacy impact assessment should be completed.

   (c) Any contract involving personal information should define personal information as defined in the *Freedom of Information and Protection of Privacy Act*.

   (d) The contract should clearly spell out that the VRHB has the custody and/or control of all personal information subject to the contract.

   (e) The contract should require the contractor and any subcontractors to agree to comply with the *Freedom of Information and Protection of Privacy Act*. In addition, the contract should include provisions for the consequences of non-compliance with the Act's requirements, including possible monetary consequences and/or contract termination. The contractor should also include provisions specifically addressing security arrangements against unauthorized access, use or disclosure, as well as provision for the disposal of personal information.

   (f) The contract should require the contractor, and any subcontractors, to appoint a senior employee, preferably at an executive level, to be responsible for privacy compliance and to be the contact for such issues. The contractor and any subcontractors should be required to train relevant employees in the requirements of the Contract and the Act and to commit, where legally permissible, to using employment discipline, if necessary, to ensure employees comply.

   (g) If there is any potential that sub-subcontractors or other third parties could have access to personal information, there should be a clause in the contract committing them to recommendation 2(e) and all other privacy provisions in the contract.

   (h) The contract should expressly stipulate, exhaustively, how, when and why the contractor, subcontractors, other third parties or sub-subcontractors can have access to personal information.

(i) The contract should include a schedule of regular and systematic audits of the contractor's and any subcontractors' compliance with the privacy provisions of the contract.

(j) In the event of the termination of the contract, the contract should also explicitly address the ability of the VRHB to demand the return of all copies of any personal information in the custody or under the control of the contractor or any subcontractor. In addition, the contract should require the contractor or any subcontractors to do what is necessary, so far as it is within their power to do so, to retrieve any copies of the personal information that fall into the hands of unauthorized persons during the contract.

[98] These contract-language recommendations are not exhaustive. The Commissioner has, in discussions about these matters generally, told me that he plans to work on revising the Office's standard contract recommendations of this kind. The Commissioner has made it clear that he believes that with the possibility of more contracting-out of services and an increase in the incidence of public-private partnerships, it is crucial that all public bodies (including the provincial government) have comprehensive, effective contract provisions addressing both privacy protection and access to information issues under the Act.

October 5, 2001

ORIGINAL SIGNED BY

Al Boyd
Portfolio Officer
Office of the Information and Privacy
Commissioner for British Columbia