



Patients First® *Patients First® is a registered trademark of the Alberta Medical Association.*

COVER LETTER

The Information and Privacy Commissioner
Office of the Information and Privacy Commissioner of Alberta
410, 9925 - 109 Street
Edmonton, Alberta T5K 2J8

I am pleased to submit the Alberta Medical Association's (AMA's) Privacy Impact Assessment regarding its implementation of an in-house billing submission service, in support of physicians providing service through AMA Physician Locum Services (PLS). Since 1992, PLS has provided Alberta physicians, practicing in eligible communities, with periods of temporary respite from practice through the provision of replacement physician service (locum physician coverage). As part of its "turnkey" service to its locum physicians, PLS submits locum physician's insured service billings to Alberta Health and Wellness.

In 2008, the operation of the PLS billing submission service was changed, from a contracted service, to an in-house service. Although the attached PIA submission is subsequent to introduction of the service change, the AMA did undertake extensive analysis, to assess risks and identify mitigation strategies related to collection, use, and disclosure of health information, prior to implementing this operational change. The AMA's analysis has now been documented and is being submitted in the form of a Privacy Impact Assessment (PIA), for review by the Information and Privacy Commissioner, and in compliance with requirements of the Health Information Act.

The PLS' in-house billing service has operated since 2008, providing insured service billing submissions, without incurring any privacy breeches. All PLS and billing service staff are keenly aware of the importance of maintaining the confidentiality of the health information entrusted to them by the information custodians, and staff strictly observe security measures to maintain this trust and confidence in the service.

The attached PIA is submitted for review and acceptance by the OIPC. As a rural physician, I utilize PLS for locum coverage, and my staff do submit locum physician's billings to the PLS Billing Service. Should there be questions about any aspects of the submission, please contact the AMA Privacy and Record staff for clarification.

Dr. David Wildeboer
Rural Physician – Lacombe, Alberta

COVER PAGE

Official Project Name: AMA Physician Locum Services Billing Service Implementation
Custodian Legal Name: Alberta Medical Association (CMA Alberta House)

Primary Contact:

Mavis A. P. Stoyko, Privacy and Records Officer
Tel: [780] 482-2626 ext. 278
Fax: [780] 482-5445
mavis.stoyko@albertadoctors.org
Alberta Medical Association
12230 106 Ave NW
EDMONTON, AB
T5N 3Z1

PIA Submission Date: February 1, 2012

Project Implementation Date: June 8, 2008

OIPC File References: none

SECTION A – PROJECT SUMMARY

What does the system or administrative practice do? The Alberta Medical Association is a not-for-profit professional membership organization incorporated under The Societies Act (1969) in the Province of Alberta. Since 1992, Alberta Medical Association (AMA) Physician Locum Services (PLS) has provided Alberta physicians practicing in eligible communities with periods of temporary respite from practice through the provision of replacement physician service (locum physician coverage). The PLS office acts as a “matching” service, collecting requests for locum coverage from practicing physicians, and advising locum physicians of the opportunity to provide medical services while physicians are away from practice. PLS coordinates required documentation for these locum coverage periods, collects patient billing information, including patient’s health information, from locum physicians, and provides payments and reimbursements to locum physicians, rural physicians and other participants as warranted.

What is the business rationale for the project? In past, PLS engaged private billing agencies, to submit insured service patient billing information to Alberta Health and Wellness, on behalf of locum physicians working with PLS. These billing submissions, and the resulting payments from Alberta Health and Wellness, form part of the locum physician’s compensation for providing locum coverage. Difficulties were identified with the cost and quality of the contracted billing submission services. An opportunity was identified to improve PLS’ billing submission and payment processes. Specifically, improvements to timeliness of submissions, quality of data submitted, data security and knowledge about the status of particular submissions were all identified as benefits of moving to an in-house billing service. Two staff members were hired as AMA employees to replace the previously contracted service.

Who are the key players? There are many key players involved in PLS’ processes of health information collection and documentation, transmission of information to AMA, and billing submission and re-submission to AHW. Parties include:

- PLS locum physicians;
- Rural family/general practice physicians (and their office staff) requesting/receiving locum coverage;
- Regional specialist physicians (and facility/office staff) requesting/receiving locum coverage;
- Alberta Health Services (AHS) care providers and administrative staff;
- Alberta Health and Wellness (AHW) staff; and
- AMA PLS staff and PLS Billing Office Staff

Where will health information be stored/accessed? Health information is received from locum physicians, their billing agents and/or physician’s offices, via:

- a confidential fax in a secured area of the office;
- electronic myfax (interfax) transmission,
- password-protected email, and/or
- via mail (i.e. Canada Post).

Receipt of patient billing information is recorded by PLS staff in the program’s computer system (MSIS), and is then hand-delivered to PLS billing service staff. While awaiting submission, patient billing records are stored in locked filing cabinets, which are located

within the secured billing service office in the AMA main office. Once the billing data is entered for submission to AHW, billing records are again stored in locked cabinets until archived at year-end. The archived records are stored for one year in AMA's on-site secure records storage repository, and are then transferred to PLS' secure, off-site records storage facility (Iron Mountain) until their retention limit is reached, at which time the documents are destroyed.

The management and storage of both hard copy and electronic records at Physician Locum Services Program Office is guided by Privacy and Security Procedure – Information Handling and Security (ATTACHMENT #1). Among other things, this policy ensures that:

- Information systems users are assigned User IDs, and access to systems is password protected;
- Data is backed up daily to the Alberta Medical Association server;
- The Alberta Medical Association server is backed up to tape weekly in an 8 tape rotation scheme and weekly back-ups must be stored in a secure off site environment;
- Identifying information is disposed of by confidential on-site shredding; and
- The destruction of non-transitory information will be documented and signed-off

An extract of the billing data is exported to MSIS (Member Services Information System). MSIS is used exclusively by Alberta Medical Association for the purpose of maintaining member's information and related member benefit details. This information includes service recipient PHN, Service Code, Date of Service, etc., as identified in Section C of this PIA document.

Locum payment information is maintained in MSIS for the purpose of fully and accurately remunerating locum physicians for service provided during their locum assignments. Payment information is also used to answer enquiries from locum physicians regarding their payments. MSIS can provide reporting to locum physicians regarding rejected claims, payments from complimentary programs (Business Costs Program (BCP), Rural Remote Northern Program (RRNP)) and other related reporting.

Why does the project need to collect, use or disclose health information to achieve its objectives? Health information is collected from locum physicians and rural physicians' offices as part of PLS' billing submission and payment process. The ***collection, use and disclosure of identifying information*** by Alberta Medical Association Physician Locum Services are governed by the provisions of the *Health Information Act (HIA)*. Locums are paid on a fee-for-service basis, and are, for payment and documentation purposes, required to document insured medical services provided. After providing medical services or consultations to patients, locum physicians (or physician office staff, on the locum's behalf) submit billings to PLS as part of the payment process. PLS receives the billing information and the PLS billing service submits billings to AHW on the locum physician's behalf. PLS uses the payments to recover an income guarantee paid to locum physicians, and subsequently pays the residual insured service amounts to the locum physician.

SECTION B – ORGANIZATIONAL PRIVACY MANAGEMENT

1. Management Structure

How is your senior management involved in decision-making related to privacy?

AMA Senior Management plays an active role in setting privacy policy and resolving privacy issues. In accordance with privacy legislation, section 4.2 of the Association's Constitution and Bylaws (ATTACHMENT #2) notes that the Executive Director is accountable for the organization's adherence to privacy legislation. As such, the Assistant Executive Director, Corporate Affairs is the Executive Director's designate for privacy and therefore serves as the Association's Chief Privacy Officer. In addition, the Privacy and Records Officer has been delegated with overseeing staff and contractor's day-to-day compliance with the organization's privacy policies, procedures, and practices, as well as training and awareness. When a privacy issue arises, the Privacy and Records Officer brings it to the attention of the Chief Privacy Officer. Depending on the specific situation, the Chief Privacy Officer may raise the issue with the Executive Director and/or the organization's Senior Management team, if warranted.

2. Policy Management

How do you develop, approve and implement privacy policies? To ensure the Association continues to meet or exceed legislative as well as organizational requirements, Senior Management worked with professionals in the field of privacy to help develop the AMA Privacy Policies and Procedures (ATTACHMENT #3). This document is periodically reviewed and revisions continue to be made since it is a living document, as is privacy legislation. Any contemplated changes are reviewed by the Chief Privacy Officer and if required, with the Executive Director and/or the organization's Senior Management team. Once any proposed changes have been approved, this document is formally updated, with staff and contractors subsequently notified via email notices. In addition, privacy policy and procedure awareness is communicated to staff and contractors during privacy training and awareness sessions.

3. Training and Awareness

How are your employees and contractors trained in privacy? Privacy training and awareness for staff and contractors consists of formal facilitator lead training sessions using a PowerPoint presentation, handouts and job-relevant examples followed by a short quiz to encourage discussion of the topics presented. The PowerPoint training is composed of modules based on the employee's level of required training. The General module covers all legislations at the basic level, while the remaining PIPA, PIPEDA and HIA modules are presented in greater depth. Currently, all staff have received job-relevant privacy training. New staff receive training within their first three months of employment. Staff are also encouraged to attend 'refresher' training as they feel the need. The employee's privacy quiz and Privacy Training Record of Attendance is placed in their HR file to serve as proof of their accountability under privacy legislation. The same documents as they relate to contractors are filed with the corresponding contractor's Services Agreement. Further, as an additional means to promote privacy awareness, several copies of the book, *The Canadian Guide to Protecting Yourself from Identity Theft and Fraud* (2007) have also been circulated which staff are encouraged to read. Finally, as legislation is amended and the media reports on any relevant privacy stories, staff and contractors are notified with email information updates and links to the media stories.

4. Incident Response – PLS investigation in cooperation with AMA Privacy Officer

How do you identify, investigate and manage privacy incidents? As soon as a breach or suspected breach involving an individual's personal (health) information comes to the attention of the organization's employees or contractors, they have learned via their privacy training to follow the steps as outlined in the attached AMA Privacy Best Practice Guideline document # 8, *Responding to Privacy Breaches* (ATTACHMENT #4). Because of the relationship we have with our members and employees, the organization operates from the viewpoint that it is best to always notify the affected parties regardless of the perceived level of harm to them. Regardless of whether a breach was found to have taken place or not, such incidents are reviewed in their entirety as a means for the organization to re-evaluate how it handles the personal (health) information in question, at which time changes may in fact be made to our personal (health) information handling practices to help improve and strengthen the systems we had in place. The organization appreciates the role that the Office of the Information and Privacy Commissioner (OIPC) plays in this regard and doesn't hesitate to contact them for assistance in how the organization handles personal (health) information.

5. Access and Correction Requests

How do you manage requests from individuals to access their own health information and to make corrections? Access and correction requests involving personal (health) information fall under the responsibility of the Privacy and Records Officer. The organization has a formal process in place to ensure it complies with the individual's information request as well as privacy legislation in a timely and organized manner. As such, this process requires that the individual complete either of the attached forms *Request to Access Information* or *Request to Correct Personal Information* (see ATTACHMENTS #5a and #5b), which is/are then date stamped and processed by the Privacy and Records Officer. Once the relevant information has been gathered, it is then reviewed for accuracy/thoroughness and shared with the individual to whom it relates. Depending on the circumstances involved, the Privacy and Records Officer may contact the OIPC for advice and assistance.

SECTION C – PROJECT PRIVACY ANALYSIS

1. Health Information Listing –

List the health information that is collected, used or disclosed in the project:

Information collected on the PLS billing templates (see ATTACHMENT #6a and #6b - PLS Patient Billing Templates: ATTACHMENT #5a - AMA Type 1 - Regular Claims Sheet and ATTACHMENT #5b - Type 2 - Person Data Segment/Text/Out-of Province claim sheet), which are completed by locum physicians and/or physician office staff, to obtain fee-for-service billing payments for locum physicians, includes

- *Patient demographic and identifying information:* surname & gender; and patient PHN; and
- *Service information:* referring physician, date of service, facility number & functional centre, encounter number, number of calls associated with the service, health service code, diagnostic code, modifiers and time/complexity units

Information collected on the billing template is in accordance with data elements required by AHW to process and make payments to physicians. *A Physician's Resource Guide* defines these data requirements (<http://www.health.alberta.ca/documents/Physician-Resource-Guide-2011.pdf>)

The locum physician generates a billing record for each patient seen at the rural physician's clinic for the purpose of submitting this record to PLS. The locum physician's treatment notes and billing information are entered in the patient record (paper or electronic) maintained by the rural physician. The locum follows the standard of practice defined by the rural physician. PLS receives the fee for service information and subsequently enters the data into Optimed EMR. The PLS Billing Service acts as an accredited submitter. As previously mentioned, the data elements submitted include:

Registration	Scheduling / Billing Information
<ul style="list-style-type: none"> • Patient name • Address • Sex • Date of birth • Physician name • Referring physician name • Personal Health Number 	<ul style="list-style-type: none"> • Appointment date • Appointment time • Amount owing • Units • Provider ID • Referring Dr. ID • Service facility • Functional centre • Date • Hospital admit date • Comments • Pay to entity • Diagnosis code(s) • Billing code(s)

The Alberta Medical Association has categorized personal information it collects as:

- Alberta Medical Association Employee Information
- Member Information (limited applicability to Physician Locum Services)
- Patient Information (as submitted via fee for service billing)

2. **Information Flow Analysis – Component #1 – Information Flow Diagram**

Diagram included in attachments – ATTACHMENT #7a – Sample Information Flow

Information Flow Analysis – Component #2 – Legal Authority and Purposes Table

Diagram included in attachments – refer to ATTACHMENT #7b - Sample Information Flow to accompany Legal Authority and Purposes Table in next section.

COMPONENT #2 – Legal Authority and Purposes Table

Information Flow (see ATTACHMENT #6b)	Description	Type of Information	Purpose	Legal Authority
#1	Collection of health information directly from patient	Patient demographic information	Treatment & payment purposes	HIA Sections 18 – 24
#2 & #3	Health information collected by PLS Office from locum/office staff	Patient demographic & service information	Payment purposes	HIA Section 27(1)(a,b) - PLS registered with AHW as billing submitter; locums added to PLS BAs
#4	PLS Billing Service collects information from PLS Office	Patient demographic & service information	Payment purposes	HIA Section 27(1)(a,b) ; 35 (1)(r)
#5	Alberta Health and Wellness (AHW) collects claims information	Patient demographic & service information	Payment purposes	HIA Section 27(1)(a,b) ; 35 (1)(r)
#6	AHW requests additional information to pay claim	Patient demographic & service information	Payment purposes	HIA Section 27(1)(a,b) ; 35 (1)(r)
#7	PLS Billing Service requests additional information from locum physician	Patient demographic & service information	Payment purposes	HIA Section 27(1)(a,b) ; 35 (1)(r)
#8	Billing Service sends copies of billing records to AMA on-site storage	Patient demographic & service information	Record Retention for possible future reference	HIA Section 27(1)(a,b) ; 35 (1)(r)
#9	PLS Office sends copies of billing records to off-site records storage	Patient demographic & service information	Record Retention for possible future reference	HIA Section 66

3. Notice

Describe how you will notify individuals of all purposes for which their health information is collected. When health information is required for billing and accredited submitter purposes, identifying information of health service practitioners, defined as custodians under the Health Information Act, will be required.

The locum physician's acknowledgement of billing information collection and use of this information is described in the contract between the locum physician and AMA Physician Locum Services, and in the guidelines that accompany the contract (ATTACHMENT #8a – Locum Physician Agreement and ATTACHMENT #8b – Rural Locum Program Guidelines). In addition, locum physicians enroll under PLS' Business Arrangement(s) allowing Alberta Health and Wellness to direct payments to PLS, for insured service claims submitted for periods of locum coverage. Pertaining to collection of health information by the rural physician's office staff on behalf of the locum physician, as a condition of a rural physician's eligibility to receive locum coverage through PLS, the custodian must acknowledge that PLS will require the billing information during the locum period for the purposes of subsequent submission to AHCIP and remuneration to the rural and locum physicians.

It is reasonable to assume that a patient who provides Alberta Health Care Insurance information to a custodian consents to its use of the information for the purposes of remuneration for services rendered. The rural physician will notify the patient primarily by way of an information poster of the collection, use, and disclosure of health information.

4. Consent and Expressed Wishes

Describe the role that individual consent plays in this project and how you will consider any wishes expressed by individuals about how much information to share. Health information collected by locum physicians, and disclosed to the PLS office and PLS Billing Service by locum physicians, is for the purpose of provision of health services. PLS submits health information to Alberta Health and Wellness as part of the process to claim payments for health services provided by the locum physician. Under the HIA, consent is not required for collection or use of health information when used for health service provision.

There is no expectation, nor any need for PLS to have direct contact with patients for the purpose of collecting personal health information.

5. Data Matching

State whether the health information from this project will be linked, matched or otherwise combined with health information from other sources. If so, describe how linkage or matching will occur and its purpose. The identifiable health information collected by locums and disclosed to PLS for billing purposes is not linked, matched or otherwise combined with health information from other sources. The data may, at times, be used at an aggregate level for trend or other analysis. None of this analysis uses data at an identifiable level.

6. Contracts and Agreements

Describe contracts or agreements with third parties involved in your project.

Describe the privacy provisions that bind third parties to your own requirements for privacy protection. Agreements are signed with third parties (e.g. Optimed Software Corporation, myfax, Iron Mountain) that provide service to PLS. Physician Locum Services may engage in contracted services both on-site and off-site to meet operational requirements of its mandate. The service contracts address the privacy, confidentiality, and security requirements of access, use and disclosure of personally identifying information and sensitive business information that the contractor may encounter. Where the AMA issues contract documents to contractors, the AMA Contractor Code of Conduct and Ethics Policy (ATTACHMENT #9) may be provided as a requirement of service. Where AMA signs another company's contract documents, review is conducted at several levels of organization to ensure there is confidence that security and privacy standards are equivalent to those required by AMA.

The PLS will engage in Information Manager Agreements with custodians (Information Manager Agreement (ATTACHMENT #10), as part of the decision by PLS to implement the best practices of the *Health Information Act* (HIA) as it relates to the privacy, confidentiality, and security expectations. Information manager agreements will be available for any rural physician or regional specialist physicians accessing PLS locum coverage. Each of the participating custodians will be responsible for completing and submitting their own amendment to this PIA to the OIPC.

7. Use of Health Information Outside Alberta

Describe how and why health information from your project is used in jurisdictions outside Alberta.

Patient's health and billing information, submitted to PLS for purposes of claiming locum physician remuneration, generally stays within Alberta's borders. The original patient treatment information is compiled, transmitted and stored by the locum physician, the locum physician's billing agent, staff in the rural physician's/specialist's office, or Alberta Health Services facility staff.

Some of the locum physicians working for PLS travel into Alberta to provide locum coverage. On occasion, these physicians may submit billings after returning home. These physicians remain as custodians of the health information they possess, and they utilize secure PLS communication channels when transmitting information to PLS: fax transmission, mail, or in a few cases, password protected email. The use of email for transmission of billing information is discouraged by PLS staff.

Billing information transmitted to or sent from the PLS fax does leave Alberta during transmission. Myfax is a service provider based in Ottawa, Ontario, with the parent company J2 Global/Protus. The company's privacy policies, data handling practices and safeguards are identified in the Protus Privacy Policy (ATTACHMENT #11 or www.protus.com/legal/privacy.asp).

The Alberta Medical Association Information Technology (IT) provides network support for the Physician Locum Services. Alberta Medical Association staff oversees the selection of equipment, installation, maintenance and secure disposal of each part of the network. AMA IT staff have reviewed the physical and software safeguards in place to protect data handled

by myfax (www.myfax.com), and have found the safeguards to be adequate; meeting or exceeding least industry standard.

Although PLS data is sent beyond Alberta's borders, the risks of a data breach have been determined to be very low. Information handled by myfax flows through the myfax information conduit. The exception to this direct and uninterrupted flow of information is a brief period of time when data is written to volatile memory during the process to convert fax data to a format which it can be sent via internet. The data in memory is overwritten once transmission has occurred. Generally, overwriting occurs in approximately five minutes. AMA has specified that no other records will be retained by myfax. In addition to data and system safeguards, there are physical safeguards at the myfax site to prevent unauthorized access to the computer system.

2. SECTION D – PROJECT PRIVACY RISK MITIGATION

1. Access Controls

Describe how persons, positions, employee categories or third parties are given access to specific health information data elements or categories.

Position, Job Title & User Role	Nature of Information Being Accessed	Circumstances Allowing Information Access	Type of Access to Information	Purpose/Reason for Access
Locum Physician (custodian)	Health Information	Examination and/or Treatment of Patient and Billing for Services Provided	Direct Access	Rendering of treatment and creation of health record
Physician Office Billing Staff -	Billing/Health Information	Preparation of billing records for services provided by locum physician	Read, write and edit access to information provided by locum physician	Creation of billing record to allow payment of locum physician
Myfax staff	Billing/Health Information	Transmission of health information via myfax transmission channel	In extremely limited circumstances, myfax staff after taking extraordinary measures, may be able to view health information during transmission from the locum physician to PLS via myfax	Outside normal staff duties and operations – health information files are normally only electronically “in-transit” through myfax
PLS Office Staff	Billing/Health Information	Information forwarded by locum or physician office	Mail/Fax - read access only; email read/edit access	Ensuring locum is registered and billing record can

		staff, to facilitate billing for service provided		be submitted; recording receipt of treatment and billing record in MSIS; searching for requested records (audit, legal requirement) in AMA on-site storage
PLS Billing Office Staff	Billing/Health Information	Submission of locum's billings to Alberta Health and Wellness	Read, entry, edit access of billing submission record	Billing submission for locum payment
Contracted Records Storage Staff	Billing/Health Information	Searching for requested records to meet legal or similar requirement	Read only (paper records)	Long-term secure storage of information as per health record retention legal requirements

2. Privacy Risk Assessment and Mitigation Plans

Describe the specific privacy risks you have identified for this project and how you plan to mitigate them.

Privacy Risk	Description	Mitigation Measures for Project	Policy Reference
Unauthorized use of information by authorized users	Accidental or intentional access to health information when not required	<ul style="list-style-type: none"> • AMA Staff Code of Conduct (ATTACHMENT #12) identifies need to safeguard confidential information. • Health Information Act and Regulations • PIPA/PIPEDA • Service contracts outlining restrictions on information collection and use 	AMA Policy – section 5 Confidential Information; and section 13 Reporting Process

		<ul style="list-style-type: none"> • Protus/myfax Privacy Policy (ATTACHMENT #11 or www.protus.com/legal/privacy.asp) • Appropriate process described in AMA Privacy Policies and Procedures 	
Unauthorized collection/use or disclosure of information by external parties	Health information sent to the wrong person during communication – wrong fax number, wrong email address.	<ul style="list-style-type: none"> • Fax – use of speed dial for PLS fax number encouraged; PLS-generated documents have correct PLS fax number for use when sending to PLS. Staff will verify fax number before sending. • Email – policy stipulates billings must be password protected; locums/senders reminded if billing are not password protected. • Privacy Breach Management Policy (ATTACHMENT #13) produced by PLS for use by clinics receiving PLS locum coverage. 	
Loss, destruction or loss of use of information	<p>Loss/destruction of information during information flow</p> <p>Loss/destruction of information while on AMA premise</p>	<ul style="list-style-type: none"> • Locum physicians normally retain copies of their billing records to check against final payments from AHW. • Billing records are securely handled and stored while awaiting entry/submission, and subsequent to entry. • Billing records are stored securely in AMA on-site storage. Storage has theft and fire protection. 	

	<p>Loss/destruction of information by contracted storage vendor</p> <p>Loss/destruction of information by contracted storage vendor</p>	<ul style="list-style-type: none"> • AMA information system, including MSIS, is backed-up routinely, allowing access to copies of stored data. • Protus has data safeguards identified in their Privacy Policy and identifies data protection and storage measures among their Terms and Conditions • Review indicates industry standard measures to safeguard information while in storage. 	
Loss of integrity of information	<p>Loss of integrity during transmission (fax/email) to AMA PLS</p> <p>Loss of information integrity by contracted storage vendor</p>	<ul style="list-style-type: none"> • Transmitted data is reviewed by PLS staff to ensure all data is received. Sender is notified if all data is not received. • Protus has data integrity protection identified among the Protus Terms and Conditions (ATTACHMENT #14) or www.protus.com/legal/terms.asp – see section #5 Data Protection and Storage of Messages) 	
Unauthorized or inappropriate collection/use or disclosure by a contractor or business partner.	Health information is utilized for an inappropriate purpose and/or disclosed by contractor	<ul style="list-style-type: none"> • Appropriate data handling and uses are described in AMA Privacy Policies and Procedures, and in contracts covering conditions and expectations for contractors, Privacy/confidentiality expectations are identified for business partners and contractors. 	AMA Policy 1.2

Other project-specific privacy risks		•	
--------------------------------------	--	---	--

3. Monitoring

Describe your plans to monitor compliance with your privacy protection measures. Include a description of the monitoring processes you will use, how frequently you will apply them, and how you will review results to improve the privacy and security of health information.

Each employee and contractor of the Physician Locum Services acknowledges in their AMA Staff Code of Conduct and Ethics Policy (ATTACHMENT #12) that their use of Physician Locum Services electronic systems may be monitored to ensure appropriate confidentiality, and security. The Physician Locum Services will pursue options to automatically generate audit logs that identify use of the system outside of office hours, same last name (of user and patient record look-up), and similar monitoring criteria.

The computer network system is monitored routinely and traffic is logged and monitored by the IT staff from the Alberta Medical Association to ensure that potential security breaches are detected and dealt with in a professional manner. Specifically, audit and access logs will be checked by the system administrator if a breach of security or privacy is suspected.

Project supervision is provided by the Physician Locum Services Program Director to ensure compliance.

PLS is working with AMA IT staff to implement a process that automatically sends an acknowledgement email to locum physicians when their billings are received. If a locum physician does not receive an email acknowledging receipt of billings, they will need to contact PLS regarding the transmission of their billings. Any suspected difficulty with transmission of health information is immediately investigated.

4. PIA Compliance

Describe how you will periodically review your PIA and provide updates or revisions to the OIPC as necessary. Also describe how you will monitor your compliance with the statements made in the PIA and make any necessary changes.

Policies, procedures and actions described in this document will be the normal operations of PLS. Any exceptions to normal operations will be followed up immediately, to ensure ongoing adherence to appropriate security procedures. When any operational changes are contemplated, they will be assessed relative to the procedures and processes outlined in this document, to ensure security of health and identifiable data is maintained.

When PLS/AMA receives notice of any change(s) of operations, terms and conditions or privacy policy by its fax provider (Protus/myfax), the identified change(s) will be assessed for their anticipated impact on the security of PLS and/or AMA data. Periodic review of Protus' Privacy Policies and Terms and Conditions will occur, to ensure awareness of any change(s), and to anticipate any consequence for PLS/AMA of the change.

PLS will coordinate its ongoing efforts with the AMA Privacy Officer to ensure adherence with existing privacy legislation, regulations, requirements and best practices. New PIAs, or amendments to this PIA will occur as appropriate.

SECTION E – POLICY & PROCEDURES ATTACHMENTS

5. Privacy Policy Table

For each topic in the table, indicate whether you have an applicable policy or procedure and, if so, the title of the document and relevant page reference(s).

GENERAL PRIVACY POLICIES			
Topic	Policy Description	Attachment Title(s)	Page Ref
Privacy Accountability	Overarching document providing organizational beliefs, orientation and direction regarding privacy, security and disclosure procedures related to sensitive and confidential information. As part of AMA, PLS is subject to, and abides by provisions of this document.	<ul style="list-style-type: none"> • AMA Privacy Policies and Procedures December 2002 rev. May 2011 (ATTACHMENT #3) 	Page 5
Access to Health Information	As part of normal operations, and since PLS is the AHW Business Arrangement(s) holder under which PLS locum physicians work, PLS receives Statements of Assessment from AHW as part of the insured service payment process. PLS does not provide access to any of this information to any parties other than the physician who provided the service, following verification of identity. In very rare circumstances, and for purposes of providing physicians with a detailed explanation of their payments for services rendered, transmission of health information to a physician may occur via fax, (password-protected) email, or mail, to fax number/address provided by the custodian physician. Other requests for health-related data	<ul style="list-style-type: none"> • AMA Privacy Policies and Procedures rev. May 2011 (ATTACHMENT #3) • Request to Access Personal Information (ATTACHMENT # 5a) • PLS Billing Data - Request to access health information should be made to the physician or Alberta Health and Wellness. AMA receives health information from these sources. 	Page 13

	must be made to AHW.		
Correction Requests	PLS has no ability to correct or otherwise manipulate health or billing information provided by AHW.	<ul style="list-style-type: none"> • AMA Privacy Policies and Procedures rev. May 2011(ATTACHMENT #3) • PLS Billing Data - Request to change health information should be made to the physician or Alberta Health and Wellness. AMA receives updated health information from these sources. 	
Training, Awareness & Sanctions	As an AMA program, PLS participates in AMA's formal privacy training program consisting of HIA, PIPA, PIPEDA. Under this training, and AMA Staff Code of Conduct and Ethics Policy (ATTACHMENT #12), staff are aware of consequences for failure to comply.	<ul style="list-style-type: none"> • AMA Privacy Policies and Procedures rev. May 2011 (ATTACHMENT #3); and AMA Staff Code of Conduct and Ethics Policy (ATTACHMENT #12) • All AMA employees receive privacy training, and sign an oath of confidentiality as part of their orientation. • Employee On Boarding Form - p.4 notes compulsory privacy training (ATTACHMENT # 23) • Privacy concerns and appropriate processes to ensure maintenance of health and member information are discussed at PLS staff meetings. • Concerns about privacy related to PLS operations are discussed with AMA privacy representatives, and are escalated to AMA Senior Management Team where appropriate. • PLS Privacy and Security Procedure – Information Handling 	Page 5

		and Security (ATTACHMENT #1)	
Collection of Health Information & Notice	As an AMA program, PLS collects health information to enable payments to locum physicians for medical services rendered.	<p>AMA Privacy Policies and Procedures rev. May 2011 (ATTACHMENT #3)</p> <ul style="list-style-type: none"> • PLS Billing Data - Under the HIA, consent is not required for collection or use of health information when used for health service provision. 	Pages 7 & 8
Use of Health Information	Health information is collected by PLS from locum physicians, for submission to AHW, to enable locum physician payment for medical services rendered.	<ul style="list-style-type: none"> • AMA Privacy Policies and Procedures rev. May 2011 (ATTACHMENT #3) • PLS Privacy and Security Procedure – Information Handling and Security (ATTACHMENT #1) 	Page 9
Disclosure of Health Information	PLS adheres to Alberta legislative policies: in some cases AHW is consulted when dealing with unusual or rare situations.	<ul style="list-style-type: none"> • AMA Privacy Policies and Procedures rev. May 2011 (ATTACHMENT #3) • Alberta Health Care Insurance Act 	Page 9
Research	PLS does not disclose health information to third parties for research purposes. Parties requesting disclosure are re-directed to other more appropriate sources of information.	<ul style="list-style-type: none"> • AMA Privacy Policies and Procedures rev. May 2011 (ATTACHMENT #3) 	
Third-Parties	PLS does not disclose health information to third parties. Parties requesting disclosure are re-directed to other more appropriate sources of information.		
Privacy Impact Assessments	PLS will undertake a PIA or PIA revision as prescribed by legislation. PLS PIAs are the responsibility of the Director PLS, with appropriate input	<ul style="list-style-type: none"> • Health Information Act and related legislation. • PLS Privacy and Security Procedure – Information Handling 	

	from other areas of AMA	and Security (ATTACHMENT #1) <ul style="list-style-type: none"> PIA Best Practice Guideline (ATTACHMENT # 24) 	
Records Retention & Disposition	PLS abides by and is governed by the AMA's Records Retention Policy. AMA IT has and follows policy to cleanse and properly dispose of drives at the end of their lifespan.	<ul style="list-style-type: none"> AMA Privacy Policies and Procedures rev. May 2011 (ATTACHMENT #3) AMA Records Retention Policy (ATTACHMENT #15) AMA Policy for Electronic Data Disposal AMA IT (ATTACHMENT #16) PLS Privacy and Security Procedure – Information Handling and Security (ATTACHMENT #1) 	Page 11
Information Classification	All health information (billing records) provided to PLS is classified by AMA as most sensitive, and is treated with the highest level of security.	<ul style="list-style-type: none"> AMA Privacy Policies and Procedures rev. May 2011 (ATTACHMENT #3) 	Introduction
Risk Assessment	PLS handles risk assessments on an ad hoc basis, and responds to identified risks as they arise.	<ul style="list-style-type: none"> PLS Privacy and Security Procedure – Information Handling and Security (ATTACHMENT #1) 	
Physical Security of Data & Equipment	PLS is subject to information security measures as required by AMA, including: <ul style="list-style-type: none"> AMA IT system and email security AMA Mobile device security Fax Physical environment safeguards including measures to protect health information from disclosure. These measures include restricted access to areas where health information is handled or stored. Storage of health information is in locked storage cabinets, in offices with locked doors. Health 	<ul style="list-style-type: none"> PLS Privacy and Security Procedure – Information Handling and Security (ATTACHMENT #1) AMA Email Usage Policy (ATTACHMENT #25) Mobile Computing Policy (ATTACHMENT #26) AMA Policy for Backup Management (ATTACHMENT #20) AMA Policy for Disaster Recovery (ATTACHMENT #21) 	

	<p>information is archived in locked storage areas with restricted access. Access to PLS office area is restricted unless PLS staff are present.</p> <ul style="list-style-type: none"> • Electronic data is stored in AMA server room, disaster recovery site and on tape at Iron Mountain. Server room is locked with access limited to key IT personnel. • The disaster recovery site is locked, with the rack also locked, and further access restrictions in place. 		
Network & Communications Security	<p>PLS is subject to network and communications infrastructure protective measures as provided by AMA</p>	<ul style="list-style-type: none"> • AMA Network Access Policy (ATTACHMENT #17) • AMA IT Password Policy (ATTACHMENT #18) • AMA Network & Zones Policy (ATTACHMENT #19) • AMA Policy for Backup Management (ATTACHMENT #20) 	
Access Controls	<p>PLS health information is only accessible by PLS office and billing service staff AMA IT Access to Information and Data Exchange Policies identified for future drafting</p>	<ul style="list-style-type: none"> • PLS Privacy and Security Procedure – Information Handling and Security (ATTACHMENT #1) 	
Monitoring & Audit	<p>PLS receives health information from custodians and provides information directly to AHW.</p>		
Incident Response	<p>A privacy incident is defined as disclosure of health information to an unintended or unauthorized party.</p>	<ul style="list-style-type: none"> • PLS Privacy and Security Procedure – Information Handling and Security (ATTACHMENT #1) 	

	The response to a privacy incident will be coordinated by the Director of Physician Locum Services, in consultation with the AMA Privacy Officer.	<ul style="list-style-type: none"> AMA Privacy Policies and Procedures rev May 2011(ATTACHMENT #3) 	
Business Continuity	As part of AMA, PLS is included under the AMA Disaster Recovery Plan	<ul style="list-style-type: none"> AMA Policy for Disaster Recovery (ATTACHMENT #21) 	
Change Control	PLS' MSIS is maintained by AMA IT staff. PLS must work with these staff, within AMA IT policies to enact any system changes.	<ul style="list-style-type: none"> AMA Change Management Policy (draft) ATTACHMENT #22 Change requests occur only through an email or call to the AMA IT Helpdesk. An AMA IT Change Form (ATTACHMENT #27) may also be required. A numbered service request ticket is created and tracked for all any change requests. This practice supports our commitment to practice due diligence. 	
PROJECT SPECIFIC POLICIES			
Project Specific Policies			

6. Previous PIA Submissions

None.

List of Attachments/possible attachments/links

PLS Privacy and Security Procedure – Information Handling and Security (ATTACHMENT #1).
Alberta Medical Association Constitution and Bylaws (ATTACHMENT #2)
AMA Privacy Policies and Procedures rev May 2011(ATTACHMENT #3)
AMA Privacy and Security Best Practice #8 – Responding to Privacy Breaches (ATTACHMENT #4)
Request to Access Information or Request to Correct Personal Information (see ATTACHMENTS #5a and #5b)
PLS Patient Billing Templates: AMA Type 1 - Regular Claims Sheet ATTACHMENT #6a and Type 2 - Person Data Segment/Text/Out-of Province claim sheet - ATTACHMENT #6b).
A Physician's Resource Guide (<http://www.health.alberta.ca/documents/Physician-Resource-Guide-2011.pdf>)
Information Flow Analysis: Component #1 – Information Flow Diagram (ATTACHMENTS #7a and #7b)
Locum Physician Agreement (ATTACHMENT #8a) and Rural Locum Program Guidelines (ATTACHMENT #8b)
AMA Contractor Code of Conduct and Ethics Policy (ATTACHMENT #9)
Information Manager Agreement Template – (ATTACHMENT #10)
Protus Privacy Policy (ATTACHMENT #11 or www.protus.com/legal/privacy.asp)
myfax webpage www.myfax.com
AMA Code of Conduct (ATTACHMENT #12)
Privacy Breach Management Policy (ATTACHMENT #13)
Protus Terms and Conditions (ATTACHMENT #14 or www.protus.com/legal/terms.asp)
AMA Records Retention Policy (ATTACHMENT #15)
AMA Policy for Electronic Data Disposal AMA IT (ATTACHMENT #16)
AMA Network Access Policy (ATTACHMENT #17)
AMA IT Password Policy (ATTACHMENT #18)
AMA Network& Zones Policy (ATTACHMENT #19)
AMA Policy for Backup Management (ATTACHMENT #20)
AMA Policy for Disaster Recovery (ATTACHMENT #21)
AMA Change Management Policy (ATTACHMENT #22)
AMA Employee On Boarding Form (ATTACHMENT #23)
AMA Privacy and Security Best Practice #7 PIA's (ATTACHMENT #24)
AMA Email Usage Policy (ATTACHMENT #25)
AMA Mobile Computing Policy (ATTACHMENT #26)
AMA IT Change Form (ATTACHMENT #27)