HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT COMPLIANCE PLAN

MELVILLE SURGERY CENTER, LLC

ADOPTION OF PLAN

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Standards for Privacy of Individually Identifiable Health Information ("Privacy Regulations") require Ambulatory Surgery Centers ("ASCs") to adopt a HIPAA Compliance Plan.

Cataract and Laser Center Partners, LLC d/b/a Ambulatory Surgical Centers of America ("ASCOA") has created a HIPAA Privacy Regulations Compliance Plan attached hereto as Schedule 1 (the "HIPAA Compliance Plan") to help ASCs affiliated with ASCOA to comply with the Privacy Regulations and HIPAA.

Melville Surgery Center, LLC hereby adopts the HIPAA Compliance Plan in its entirety and intends to appoint a Privacy Official/Security Official and take all steps indicated in the plan, as are appropriate and applicable.

ADOPTED AND ACKNOWLEDGED
this _____ day of _____, _____.

MELVILLE SURGERY CENTER, LLC

_____
Signature

Name: _____

Its: _____

Created on 6/3/2009
\8023865.7

SCHEDULE 1

CATARACT AND LASER CENTER PARTNERS, LLC D/B/A AMBULATORY SURGICAL CENTERS OF AMERICA
HIPAA PRIVACY REGULATIONS COMPLIANCE PLAN

Cataract and Laser Center Partners, LLC d/b/a Ambulatory Surgical Centers of America (the "Company") has established this compliance plan (this "Plan") to ensure that the ambulatory surgical centers that it manages (collectively referred to as the "ASCs" and each individually referred to as the "ASC") comply with the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Regulations") promulgated under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the HIPAA Security Rule Standards ("Security Rule").

Compliance with the Privacy Regulations and the Security Rule is important because failure to comply is a criminal violation and can lead to serious financial and/or criminal liability for individuals and organizations.

This Plan is not intended to be a comprehensive explanation of the Privacy Regulations and the Security Rule, nor will it provide answers to every possible issue that may arise under the Privacy Regulations and the Security Rule. Rather, it is intended to provide guidelines with respect to the steps that the ASCs must take in order to achieve compliance with the Privacy Regulations and the Security Rule and to sensitize the ASCs to potential problems that may arise under the Privacy Regulations and the Security Rule. The Company and the ASCs expect full compliance with the guidelines set forth in this Plan, and encourage their members and employees to seek any further necessary information or clarification prior to engaging in any potentially sensitive actions or activities. This Plan does not address the laws of the various states in which the ASCs are located which relate to the use and disclosure of patient health information. As such, in addition to complying with this Plan, Privacy Regulations and the Security Rule, each ASC shall take all steps necessary to comply with all laws of the state in which the ASC is located relating to patient health information, including contacting legal counsel when the ASC is unsure of how to comply with such laws.

This Plan is divided into five main sections: (1) an overview of the Privacy Regulations; (2) specific compliance guidelines for the Privacy Regulations; (3) an overview of the Security Rule; (4) specific compliance guidelines for the Security Rule; and (5) National Provider Identifier guidelines. This Plan requires each of the ASCs to:

1. Appoint a Privacy Official/Security Official;

2. Form a HIPAA Compliance Committee;

3. Inform patients of the ASC's privacy practices by disseminating a Privacy Notice and obtaining patients' acknowledgement of receipt of the Privacy Notice;

4. Use a patient authorization and consent;

5. Use Business Associate agreements;

6. Provide patients with notification when their unsecured protected health information has been breached;

7. Maintain a log that tracks disclosures of a patient's protected health information when such disclosure is not exempt from tracking and, upon request, provide a patient with an accounting of such disclosures;

8. Clarify discipline for employees and vendors who violate the Privacy Regulations, the Security Rule, this Plan, the ASC's Privacy Policies and Procedures and the ASC's Security Rule Policies and Procedures;

9. Update this Plan and the Privacy and Security Policies and Procedures as needed;

10. Hold all-employee educational meetings;

11. Discuss adoption of this Plan, the Privacy Policies and Procedures and the Security Rule Policies and Procedures at a Board Meeting;

12. Develop safeguards to protect and de-identify Protected Health Information (as defined in the regulations).

SECTION 1: OVERVIEW OF THE PRIVACY REGULATIONS

Congress enacted HIPAA in 1996, in part, to provide for the regulation of the privacy of health information and the simplification of administration of health insurance. The Secretary of Health and Human Services ("HHS") published the Privacy Regulations pursuant to HIPAA on December 28, 2000, 65 Fed. Reg. 82462, 45 CFR Parts 160 and 164. The Secretary then issued significant modifications to the regulations, which were published in the Federal Register on August 14, 2002, 67 Fed. Reg. 53181.

The Privacy Regulations became effective on April 14, 2001, and the final modifications to the Privacy Regulations became effective on October 15, 2002. The Health Information Technology for Economic Clinical Health Act (the "HITECH Act"), passed February 17, 2009, made further changes to the Privacy Regulations.

The Privacy Regulations set forth certain protections that health plans, health care clearinghouses, and health care providers ("Covered Entities") must implement in their use and handling of all medical records and other individually identifiable health information, which is in any form, whether electronic, on paper or oral, and which is held or transmitted by a Covered Entity ("Protected Health Information" or "PHI"). The Privacy Regulations' protections are designed to guard against the misuse or unauthorized disclosure of patients' health records and medical information. ASCs are Covered Entities, and therefore must comply with the regulations.

Penalties for non-compliance range from a fine of $100 per person, per incident for unintentional prohibited disclosures (which can total up to $25,000 per person per year) up to a

fine that could total $1,500,000 for instances of uncorrected willful neglect. Non-compliance can also result in jail time for violators.

SECTION 2: COMPLIANCE GUIDELINES

I. Privacy Official

Each of the ASCs' HIPAA Compliance Committees shall appoint a Privacy Official. The Privacy Official shall report to the HIPAA Compliance Committee and oversee this Plan. The Privacy Official at each ASC shall be responsible for:

1. developing, implementing and maintaining this Plan and the ASC's Privacy Policies and Procedures;

2. overseeing and monitoring the ASC's HIPAA Privacy Regulations compliance activities;

3. maintaining compliance;

4. ensuring that this Plan and the Privacy Policies and Procedures are kept current and are followed by all employees;

5. distributing this Plan and the Privacy Policies and Procedures to all employees who handle or use PHI;

6. serving as the ASC's contact person to answer questions and receive complaints regarding the ASC's PHI practices and compliance with the Privacy Regulations;

7. developing and implementing training programs for all employees, as described in Section III.L.;

8. performing periodic assessments of the ASC's privacy risks to determine the need for modification to the ASC's Privacy Policies and Procedures;

9. coordinating with legal counsel and the HIPAA Compliance Committee to develop and maintain appropriate authorization forms, Privacy Notice and Business Associate Agreements;

10. managing procedures for the release of patient information, resolution of patient privacy disputes and requests for changes to medical records;

11. overseeing the development, implementation and ongoing compliance monitoring of Business Associate Agreements;

12. establishing processes for tracking and reporting disclosures of PHI and providing access to patients to inspect and copy their medical records; and

13. performing other functions as specified throughout this Plan.

II. HIPAA Compliance Committee

A Compliance Committee comprised of experienced, senior level employees and Members of each of the ASCs, will convene at least quarterly. The Privacy Official will chair the Compliance Committee. The Compliance Committee at each ASC will be responsible for:

1. working with the Privacy Official to develop the ASC's Privacy Policies and Procedures;

2. reviewing, in conjunction with counsel, new or modified HIPAA regulations and related federal and state laws pertaining to patient privacy to determine if modifications to the Privacy Policies and Procedures are needed;

3. recommending and monitoring, in conjunction with the Privacy Official, the development of internal systems and controls to carry out this Plan and the Privacy Policies and Procedures; and

4. inventorying all business partners that have access to PHI, analyzing current contracts and negotiating with Business Associates to enter into Business Associates Agreements or include appropriate language in existing contracts to ensure protection of PHI.

III. Standards and Procedures

Each of the ASCs shall adhere to the following standards. In addition, the Privacy Official shall develop and implement written compliance policies and procedures (the "Privacy Policies and Procedures") to supplement these standards where appropriate. This Plan and the Privacy Policies and Procedures shall be distributed to all employees and Members of each ASC.

A. Safeguards

The ASC shall develop and implement administrative, technical and physical safeguards (a) to protect the privacy of PHI against any intentional or unintentional disclosure in violation of the Privacy Regulations, this Plan or the ASC's Privacy Policies and Procedures, and (b) to limit incidental uses or disclosures made pursuant to otherwise permitted or required uses and disclosures.

B. Written Consent

The ASC shall make a good faith effort to obtain the written consent (an example is attached hereto as Exhibit A) of each of its patients before using or disclosing the patient's PHI for purposes of treatment, payment, and health care operations, as permitted under the Privacy Regulations and described more fully below in Section C. The ASC shall present the consent to each of its patients, accompanied by a Notice (as described in Section F) that contains a detailed discussion of the ASC's health information privacy practices. The consent shall serve as the

patient's acknowledgement of his or her receipt of the ASC's Notice of privacy practices, as required under the Privacy Regulations and as more fully described in Section III.F.3.

C. Uses and Disclosures

The ASC shall use and disclose PHI only as permitted or required by the Privacy Regulations.

1. Required Disclosures

The ASC shall disclose PHI, but need not obtain the patient's written authorization, as described in Section III.E., when requested to do so by the following:

(a) to a patient who is the subject of the information; and

(b) to HHS for enforcement of the Privacy Regulations.

2. Permitted Disclosures

The ASC may use and disclose a patient's PHI without obtaining the patient's written authorization, as described in Section III.E., for the following purposes:

(a) Treatment. The ASC may use or disclose to another provider a patient's PHI for the provision, coordination, or management of health care, including consultations and referrals between health care providers within the ASC and outside the ASC.

(b) Payment. The ASC may use or disclose to another provider or Covered Entity a patient's PHI for reimbursement or eligibility of insurance benefits purposes or in connection with billing, claims management, "medically necessary" determinations, or utilization review. However, effective February 17, 2010, the ASC must grant a patient's request to restrict disclosure of PHI for payment purposes if the disclosure is to a health plan and the PHI pertains solely to a health care item or service for which the ASC has been paid out of pocket in full.

(c) Health Care Operations. The ASC may use PHI in connection with quality assessment and improvement activities, case management and care coordination, review of the competence of qualifications of health care professionals, arranging for legal services, underwriting, business planning, customer services, and resolution of internal grievance and other operational activities set forth in the Privacy Regulations. If the ASC discloses PHI to another Covered Entity for that entity's health care operations, however, the entity must have a relationship with the patient, the disclosure must pertain to the relationship, and the reason for the disclosure must relate to the entity's quality assessment and improvement activities or its review of the competence or qualifications of a health care professional. Additionally, effective February 17, 2010, the ASC must grant a patient's request to

restrict disclosure of PHI for health care operations purposes if the disclosure is to a health plan and the PHI pertains solely to a health care item or service for which the ASC has been paid out of pocket by the patient in full.

(d) Appointment Reminders. The ASC may use PHI to remind patients of appointments for treatment or medical care at the ASC.

(e) Treatment Alternatives. The ASC may use PHI to contact patients about or recommend possible treatment options or alternatives that may be of interest to patients.

(f) Health-Related Benefits and Services. The ASC may use PHI to inform patients about health-related benefits or services that may be of interest to them.

The ASC may use a patient's PHI without the patient's written authorization as described in Section III.E. for the following purposes, but only if it first informs the patient that it will use or disclose the PHI for the stated purpose and provides the patient with an opportunity to agree to, restrict or object to the disclosure or use:

(a) Individuals Involved in the Patient's Care or Payment for Care. The ASC may release medical information about a patient to a friend or family member or other persons identified by the patient who are involved in the patient's medical care or who help pay for the patient's care.

(b) Notification. The ASC may use or disclose a patient's medical information to notify or assist in notifying a family member, personal representative, or other person responsible for the patient's care of the patient's location and general condition.

The Privacy Regulations permit the ASC to use or disclose PHI without first obtaining the patient's authorization in a variety of other contexts when certain conditions are met. These situations include the following: (a) as required by law; (b) pursuant to laws relating to workers' compensation; (c) for public health risks purposes; (d) to comply with the activities of a health oversight agency; (e) pursuant to requests made in connection with law suits; (f) for law enforcement purposes; (g) to the Food and Drug Administration; (h) to report victims of abuse, neglect or domestic violence; (i) to report child abuse or neglect; (j) to avert a serious threat to the health or safety of a patient or other person; (k) to organ procurement organizations; (l) to a coroner or medical examiner or funeral director; (m) when the information relates to a patient who is an inmate; (n) for fundraising purposes so long as any written fundraising communication sent after February 17, 2010 clearly provides an opportunity for the recipient to opt-out of any such further communications; and (o) for patient directories. The ASC shall consult with the Privacy Regulations or legal counsel where appropriate when unsure of how and when to use or disclose PHI in these situations.

3. Restricted Records

State and Federal laws impose specific requirements on the disclosure of patient medical records that relate to HIV status, drug and alcohol abuse treatment, and psychotherapy notes. The ASC shall consult with such laws or legal counsel when required to disclose patient health information relating to such topics.

D. Minimum Necessary

The ASC shall limit the access, use, disclosure, and its request of PHI, to the extent practicable, to the limited data set as defined below, or, if needed by the ASC, to the minimum extent necessary to accomplish the intended purpose.

A limited data set is PHI that excludes the following direct identifiers of the patient or of the relatives, employers or household members of the patient: (a) names; (b) postal address information, other than town or city, State and zip code; (c) telephone numbers; (d) fax numbers; (e) email addresses; (f) social security numbers; (g) medical record numbers; (h) health plan beneficiary numbers; (i) account numbers; (j) certificate/license numbers; (k) vehicle identifiers and serial numbers, including license plate numbers; (l) device identifiers and serial numbers; (m) Web Universal Resource Locators (URLs); (n) Internet Protocol (IP) address numbers; (o) biometric identifiers, including finger and voice prints; and (p) full face photographic images and any comparable images.

Accordingly, the ASC may not request, use or disclose the entire medical record of a patient unless the ASC makes a determination that the entire medical record is specifically justified as the amount of information that is the minimum necessary to accomplish the specified purpose.

In order to comply with this requirement, the ASC shall implement policies and procedure regarding the following.

1. Workforce

The ASC shall identify persons or classes of persons in its workforce who need access to PHI to carry out their duties and the category or categories of PHI to which such person need access. Once the persons/categories have been determined, the ASC shall limit the access of such persons to the categories of PHI that they need in order to carry out their duties.

2. Routine Disclosures and Requests of PHI

The ASC's disclosures and requests for PHI that are made on a routine and recurring basis shall be made in accordance with standard protocols that limit the disclosure or request of PHI to the limited data set, or, if needed, the minimum amount necessary to achieve the purpose of the disclosure or request.

3. Non-Routine Disclosures and Requests of PHI

All non-routine disclosures of or requests for PHI shall be reviewed on an individual basis to ensure that only the limited data set, or, if needed, the minimum amount of PHI necessary to accomplish the intended purposes is requested or disclosed.

4. Presumed Minimum Necessary

The ASC may presume that certain disclosures or requests which are made to the following persons or entities meet the minimum necessary requirement if such persons or entities represent that such request or disclosure will be limited to the limited data set, or, if needed, the minimum amount of PHI necessary for the stated purposes: (i) public officials requesting PHI that is required to be disclosed by law; (ii) another covered entity; or (iii) a professional who is a member of the ASC's workforce or is a Business Associate of the ASC for the purpose of providing professional services to the ASC.

The ASC need not adhere to the minimum necessary requirement when: (a) disclosing PHI to or requesting PHI from another health care provider for treatment purposes; (b) disclosing PHI to patients pursuant to their own request; (c) disclosing PHI to the Secretary of HHS for overseeing compliance of the Privacy Regulations; (d) using or disclosing PHI pursuant to an authorization; or (e) using or disclosing PHI as required by law.

The Secretary of HHS will issue guidance on the minimum necessary requirement by August 17, 2010. The ASC will comply with this forthcoming guidance by its effective date and issue notifications regarding the same to its employees, Members, officers and agents.

E. Authorization

The ASC shall use an authorization (an example is attached hereto as Exhibit B) that allows it or a third party to use and disclose PHI for purposes not listed above in Section III.C. The authorization shall be written in plain language and in specific terms. The authorization shall include:

1. a description of the PHI to be used or disclosed and the purpose of the use or disclosure;

2. the name of the person (or class of persons) who is authorized to make the use or disclosure of the PHI;

3. the name of the person (or class of persons) who is authorized to receive the PHI;

4. an expiration date or an event upon which expiration of the authorization occurs;

5. a notice of the patient's right to revoke the authorization in writing and instructions on how the patient may revoke the authorization;

6. an explanation that the PHI, if used or disclosed, may be subject to redisclosure by the recipient and is no longer protected by the Privacy Regulations;

7. a notice that if a patient revokes the authorization, the ASC shall honor such revocation, except to the extent that it has used or disclosed the information in reliance on the authorization; and

8. the individual's signature and date of signature.

F. Notice

1. Content

The ASC shall make available to its patients a written notice (the "Notice") (an example is attached hereto as Exhibit C), detailing the ASC's health information privacy practices. The notice shall contain a header that reads: "**THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY**." The notice shall contain the following information:

(a) A description of the patient's rights with respect to his or her PHI and how the patient may exercise those rights;

(b) The duties of the ASC under the Privacy Regulations, this Plan and the Privacy Policies and Procedures;

(c) A description of the types of uses and disclosures of PHI that are permitted under the Privacy Regulations and the ASC's Privacy Policies and Procedures, including those uses and disclosures that are permitted or required without the patient's written authorization;

(d) An explanation of how the patient can file a complaint with the ASC and the Secretary of HHS;

(e) An explanation of how the ASC will provide the patient with a revised Notice if it revises the Notice;

(f) The name of the person at the ASC who can be contacted for additional information regarding the ASC's privacy practices; and

(g) The effective date of the Notice.

2. When and How to Provide Notice

The ASC shall:

(a) post the notice conspicuously in its waiting area;

(b) provide a copy to each patient, new or existing, as of the date of the first service delivery after the compliance date, or in emergency situations, as soon as reasonably practicable after the emergency treatment situation; and

(c) provide additional copies and any revisions to the Notice to patients upon request.

3. Written Acknowledgement of Patients' Receipt of Notice

The ASC shall obtain a written statement (in the form of the Written Consent attached hereto as Exhibit A) from each patient, in which the patient acknowledges that he or she received a copy of the ASC's Notice. If the ASC is unable to obtain the acknowledgement from a particular patient, it shall document the efforts that it made to obtain the acknowledgement and the reason why the acknowledgement was not obtained.

4. Revisions to the Notice

If the ASC revises its Notice, it shall provide patients with the new Notice before the changes are actually implemented.

G. Marketing

The ASC shall obtain a patient's authorization, as described in Section III.E., before using the patient's PHI for marketing purposes or before selling its patient list to a third party for the third party's marketing purposes. The authorization shall disclose to the patient whether the ASC will receive direct or indirect remuneration for the disclosure. Marketing includes communications that encourage the patient to purchase or use a product or service.

The ASC may use PHI for marketing purposes without the patient's authorization, however, if:

(a) the marketing occurs face-to-face; or

(b) the marketing involves a promotional gift of nominal value.

Marketing does not include, and therefore the ASC need not obtain the patient's authorization before using his or her PHI for communications describing or made for:

(a) a health-related product or service that is provided by the ASC;

(b) the ASC's participation in a provider or plan network;

(c) treatment of the patient;

(d) the case management or coordination of care of the patient; and

(e) the direction or recommendation of alternate therapies, providers, or settings of care.

These exempted communications described immediately above, however, will be considered marketing for which patient authorization is required as of February 17, 2010 if the

ASC has received direct or indirect remuneration in exchange for making such communication unless one of the following applies:

(a) the communication describes only a drug or biologic that is currently being prescribed for the patient and any payment received by the ASC in exchange for making the communication is reasonable in amount; or

(b) the communication is made by a business associate of the ASC and the communication is consistent with the business associate agreement between the business associate and the ASC.

H. Sale of PHI

The Secretary will issue guidance no later than July 17, 2010 that places certain restrictions on the sale of PHI. This guidance will become effective 6 months after issuance, and the ASC shall comply with this guidance by its effective date. The guidance will restrict the ability of the ASC to directly or indirectly receive remuneration in exchange for the PHI of a patient unless the ASC obtains a valid authorization from the patient. Patient authorization is not needed, however, if the purpose of the exchange is for: (a) public health activities; (b) research; (c) treatment of the patient; (d) health care operations; (e) remuneration provided to a business associate for activities undertaken by it pursuant to a business associate agreement, or (f) providing a patient with a copy of his or her PHI.

I. Patient Access to PHI

1. Content

The ASC shall provide patients the opportunity to see and obtain a copy of their own PHI which is contained in the ASC's medical and billing records, including electronic health records, in any form or format requested by the patient. The ASC may provide the patient with an explanation or summary of the requested PHI if the patient agrees in advance to the arrangement and the fees imposed. If the ASC no longer maintains the patients PHI, but knows where the information is kept, the ASC shall inform the patient where the information can be located.

Effective February 17, 2010, the ASC shall transmit a copy of a patient's electronic health records directly to any entity or individual designated by the patient, provided that the patient's request that the ASC do so is clear, conspicuous and specific.

2. Time Frame

The ASC shall provide the information to the patient within thirty (30) days of receiving the request, or sixty (60) days if the ASC does not maintain or have access to the information on-site. The ASC may extend this time period by thirty (30) days if it provides the patient with a written statement explaining the reasons for the delay and indicating the date by which it will fulfill the request.

3. Cost

The ASC may charge the patient reasonable, cost-based fees for providing the patient a copy, explanation, or summary of his or her PHI. If the information is provided in electronic form, the ASC may not charge the patient more than the ASC's labor costs in responding to the request.

4. Denial of Access

The ASC may deny a patient access to all or part of his or her PHI without providing the patient an opportunity for review of the denial if the PHI constitutes one of the following:

(a) psychotherapy notes;

(b) PHI compiled in anticipation of or for use in a civil, criminal or administrative action or proceeding;

(c) PHI maintained by the ASC that is subject to Clinical Laboratory Improvement Amendments (CLIA) or exempt from CLIA regulations;

(d) PHI requested by an inmate, if providing a copy to the inmate would jeopardize the health, safety, security, custody or rehabilitation of the inmate or other inmates, or the safety of any officer, employee or other person at the correctional institution;

(e) PHI that relates to treatment for research purposes, if certain conditions are met;

(f) PHI that is contained in records that are subject to the Privacy Act, 5 U.S.C. 5a, if access under the Privacy Act would meet the requirements of that law; or

(g) PHI that is obtained by the ASC under a promise of confidentiality and access would reasonably likely reveal the source of that information.

The ASC may deny a patient access to all or part of his or her PHI if the ASC provides the patient an opportunity for review of the denial by a licensed health care professional who was not involved in the initial decision, under the following circumstances:

(a) A licensed health care professional, in the exercise of professional judgment, determines that it is reasonably likely that access to the requested PHI would endanger the life or physical safety of the patient or another person;

(b) The PHI makes reference to another person (except other health care providers) and the licensed health care professional, in the exercise of professional judgment, determines that access is reasonably likely to cause substantial harm to that other person; or

(c) The request for PHI is made by the patient's personal representative, and a licensed health care professional, in the exercise of professional judgment,

determines that providing access to that representative is reasonably likely to cause substantial harm to the patient or another person.

The ASC shall provide written notice to the patient of its decision to deny the request, the reason for the denial, and an explanation of the patient's right to have the denial reviewed.

J. Amendment to PHI

1. General Right

The ASC shall provide patients the opportunity to amend or supplement their own PHI. If the ASC accepts the request, it shall make the appropriate amendment and inform the patient in a timely fashion that the amendment was made. The ASC shall provide the amendment to the entities identified by the patient and other entities that the ASC knows have received the erroneous information.

2. Time Frame

The ASC shall act on the request for amendment no later than sixty (60) days after the receipt of the patient's request. The ASC may extend this time period by thirty (30) days if it provides the patient with a written statement explaining the reasons for the delay and indicating the date by which the request will be fulfilled.

3. Denial of Request

The ASC may deny a patient's request for amendment if it determines that the information or record:

(a) Was not created by the ASC, unless the originator of the PHI is no longer available to make the amendment;

(b) Is not part of the medical or billing records of the patient;

(c) Would not be available for inspection (i.e., the patient would not have access to the information as indicated above in Section III.H.); or

(d) Is accurate and complete.

If the ASC denies the patient's request, it shall provide the patient in a timely manner with a written statement of the denial which includes: (a) the basis for the denial; (b) the patient's right to submit a written statement disagreeing with the denial and how to exercise the right; (c) a statement that the patient can request that the ASC include the patient's request and the denial with any future disclosures of the PHI (if the patient does not file a statement of disagreement); and (d) a description of how the patient can file a compliant with the ASC or the Secretary of HHS. The ASC may prepare a rebuttal to the patient's statement. The request for amendment, the denial, the statement of disagreement (if submitted), and the rebuttal (if any), or a summary of such information shall be provided with any subsequent disclosures of the patient's PHI.

K. Accounting for Disclosures

1. Content of Accounting

The ASC shall provide upon a patient's request an accounting of disclosures of the patient's PHI made by the ASC during the six (6) years (or shorter period as requested by the patient) prior to the date that the patient requested the accounting. The accounting shall include the following information: (a) the date of each disclosure; (b) the name and, if known, the address of the entity or person to whom the disclosure was made; (c) a description of the information disclosed; and (d) a statement of the purpose of the disclosure.

The ASC shall include in the accounting all disclosures made to other entities and persons outside the ASC, including disclosures made to or by Business Associates. However, the following disclosures need not be included in the accounting: (a) disclosures for treatment, payment or healthcare operations; (b) disclosures made to the patient; (c) disclosures made pursuant to the patient's authorization; (d) disclosures made incident to an otherwise permitted disclosure; (e) disclosures made for the ASC's directory or to person's involved in the patient's care or other notification purposes; (f) disclosures made pursuant to national security or intelligence purposes; (g) disclosures made prior to the compliance date; and (h) certain disclosures made for research purposes.

Beginning within the next several years, the ASC will be required to track and, upon request, provide an accounting of all disclosures of a patient's PHI, including disclosures for treatment, payment or healthcare operations if such disclosures are made through an electronic health record. The ASC will be required to provide an accounting for the three (3) year period prior to the date that the patient requests the accounting, provided, however, that the ASC will not be required to begin tracking any such disclosures until the applicable effective date as described below.

These changes to the HIPAA disclosure tracking and accounting requirements are scheduled to take effect within the next several years. If the ASC currently uses electronic health records, these standards will change as early as January 1, 2014 and as late as January 1, 2016. If the ASC has not yet acquired electronic health records, these standards will change as early as January 1, 2011 or as late as January 1, 2013. These standards will only apply to ASCs that have acquired electronic health records, so they will not become applicable to an ASC until it has done so. The effective date of these changes will be determined by the Secretary of HHS, who will issue guidance on these changes prior to any effective date. The ASC will implement these changes and comply with the guidance.

2. Time Frame

The ASC shall provide the accounting no later than sixty (60) days after the receipt of the patient's request. The ASC may extend this time period by thirty (30) days if it provides the patient with a written statement explaining the reasons for the delay and indicating the date by which it will provide the accounting.

The ASC shall provide the first accounting provided to the patient in any twelve (12) month period at no charge. The ASC may charge the patient reasonable, cost-based fees for additional accountings in the same twelve (12) month period, provided the ASC informs the patient of the fee in advance and provides the patient an opportunity to withdraw or modify the request in order to avoid or reduce the fee.

3. Cost

The ASC must provide the first accounting provided to the patient in any twelve (12) month period at no charge. The ASC may charge the patient reasonable, cost-based fees for additional accountings in the same twelve (12) month period, provided the ASC informs the patient of the fee in advance and provides the patient an opportunity to withdraw or modify the request in order to avoid or reduce the fee.

L. Notification in Case of Breach

Effective on or about September 17, 2009, the ASC shall provide patients with notification in the event that the ASC discovers that a patient's unsecured PHI has been, or is reasonably believed to have been, accessed, acquired or disclosed as a result of a breach. Notification shall be provided by the ASC to the patient without unreasonable delay and in no case later than 60 days after the discovery of the breach. Notification may be delayed if a law enforcement official determines that notification would impede a criminal investigation or cause damage to national security.

A breach will be defined as the unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of the PHI, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

The following, however, shall not be considered a breach:

(a) Any unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of the ASC if such acquisition, access or use was made in good faith and within the course of scope of employment or other professional relationship and such information is not further acquired, accessed, used or disclosed by such person; or

(b) Any inadvertent disclosure from an individual who is otherwise authorized to access PHI at the ASC or its Business Associate to another similarly situated individual at the same entity and such information is not further acquired, accessed, used or disclosed by such person.

Unsecured PHI will be defined as either:

(x) PHI that is not secured through the use of a technology or methodology as specified in guidance issued by the Secretary of HHS no later than April 17, 2009; or

(y) If the Secretary of HHS fails to issue such guidance by that date, as PHI that is not secured by a technology standard that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

A breach will be considered discovered by the ASC as of the first day on which the breach is known or reasonably should have been known to the ASC, an associate of the ASC (including its employees, officers, or agents).

If the notification is to an individual patient, notice must be provided by first-class mail at the patient's last known address, unless the patient has expressed a preference that he or she be contacted by the ASC by email. If the ASC has insufficient or out-of-date contact information for the patient that precludes direct written or electronic communication, substitute notification shall be permitted. If the ASC is required to notify 10 or more patients for which there is insufficient contact information, the ASC must make a conspicuous posting on the home page of the ASC's website or publish notice in major print or broadcast media in geographic areas where the patients affected by the breach are likely to reside. If the ASC deems that notification of the breach requires urgency due to possible imminent misuse of the PHI, the ASC may provide notification to the patient by phone.

If the ASC discovers a breach of unsecured PHI for more than 500 patients who reside in the ASC's home State, the ASC shall provide notice to prominent media outlets serving the State.

The notification of breach provided to patients shall, to the extent possible, include the following information regardless of whether the notification is provided in written form, through a website, or through written, radio or televised media:

(a) A brief description of the incident, including the date of the breach and the date of the discovery of the breach;

(b) A description of the types of unsecured PHI that were involved (e.g. full name, date of birth, home address, account number);

(c) The steps the patient should take to protect themselves from potential harm resulting from the breach;

(d) A brief description of what the ASC is doing to investigate the breach, to mitigate losses, and to protect against any further breaches; and,

(e) Contact procedures for patients to ask questions or learn additional information, including a toll-free telephone number, an email address, a website, or a postal address.

The ASC shall also provide notice of breach of any unsecured PHI to the Secretary of HHS. If the breach was with respect to 500 or more patients, notice must be provided to the

Secretary immediately. If the breach was with respect to less than 500 individuals, the ASC may maintain a log of any such breaches and annually submit the log to the Secretary.

M. Business Associates

The ASC shall enter into a contract (a "Business Associate Agreement") (an example is attached hereto as Exhibit D) with all of its business associates who may come into contact with PHI such as data processing, administrative services or billing services ("Business Associates"). Business Associates include any person or corporation that uses PHI *on behalf* of the ASC. For example, when the ASC discloses PHI to health plans for payment purposes, no business associate relationship is established. While the ASC may have an agreement to accept discounted fees as reimbursement for services provided to health plan members, neither entity is acting on behalf of or providing a service to the other. Business Associates also include any organization that provides data transmission of PHI to the ASC and that requires routine access to such PHI, including health information exchange organizations, regional health information organizations, e-prescribing gateways, and any vendor that the ASC contracts with to offer a personal health record to patients.

The ASC may disclose PHI to a Business Associate and may allow a Business Associate to create or receive PHI on its behalf, so long as the ASC obtains satisfactory assurance, in the form of a written contract, that the Business Associate will appropriately safeguard the information by complying with the requirements of the Privacy Rule and Security Rule that are applicable to Business Associates.

The Business Associate contract shall contain provisions whereby the Business Associate agrees to:

(a) abide by the ASC's Privacy Policies and Procedures and this Plan;

(b) not use or further disclose the PHI except as permitted by law;

(c) implement and use appropriate safeguards to prevent the unauthorized use and disclosure of PHI and to comply with the law;

(d) make available PHI upon patient request and for amendment purposes;

(e) report to the ASC any use, disclosure or breach of PHI not provided for in its contract with the ASC;

(f) make available the information required to provide an accounting of disclosures;

(g) make its books and records relating to PHI received from the ASC available to the Secretary of Health and Human Services for purposes of determining the ASC's compliance with the Privacy Regulations;

(h) ensure that any agents, including subcontractors, to whom it provides PHI which was received from the ASC or generated on behalf of the ASC, agrees

to the same restrictions and conditions that apply to it with respect to such information; and

(i) at termination of the contract with the ASC, if feasible, return or destroy all PHI received from, or created or received by the Business Associate on behalf of, the ASC.

N. Educational and Training Programs

All ASC employees shall attend training and educational programs periodically for updates on new developments with respect to the Privacy Regulations, this Plan or the Privacy Policies and Procedures. These programs shall be designed to:

1. teach employees what practices and procedures are required under the Privacy Regulations and what procedures should be used under this Plan;

2. emphasize the ASC's commitment to compliance with the Privacy Regulations; and

3. reinforce to employees that strict compliance with the Privacy Regulations, this Plan and the Privacy Policies and Procedures is a condition of employment.

New ASC employees shall be provided training with respect to the Privacy Regulations, this Plan and the ASC's Privacy Policies and Procedures within reasonable time after hire.

O. Employee/Business Associate Sanctions

Strict compliance with the Privacy Regulations, this Plan and the Privacy Policies and Procedures is a condition of an employee's employment with the ASC or of a Business Associate's business with the ASC. Accordingly, the ASC shall sanction employees, Business Associates and agents who violate the Privacy Policies and Procedures, this Plan or the Privacy Regulations.

P. Complaints

The ASC shall develop policies and procedures that provide for a process by which individuals may file complaints regarding the Privacy Policies and Procedures and this Plan or compliance therewith.

Q. De-Identify Information

The ASC shall adopt a policy to encourage the deletion of all identifying information from PHI before transmission in order to allow the ASC to use and disclose the de-identified information.

Because properly de-identified information is not subject to the requirements of the Privacy Regulations unless it is re-identified, the ASC may use PHI to create information that is

not individually identifiable health information or disclose PHI to a Business Associate for such purposes, whether or not the de-identified information is to be used by the ASC.

R. Uses and Disclosures Required by Law

The ASC may use or disclose PHI in order to comply with laws requiring the use or disclosure of PHI, provided the use or disclosure meets and is limited to the relevant requirements of such other laws. "Required by law" means a mandate contained in a law that compels an ASC to make a use or disclosure of PHI and that is enforceable in a court of law. Examples include court-ordered warrants and subpoenas issued by a court. It does not include contracts between private parties or similar voluntary arrangements. The ASC need not make a use or disclosure required by the legal demands or by any other law or legal process, and may challenge the validity of such laws and processes. The ASC shall contact counsel any time it considers disclosing PHI pursuant to this Section.

S. Written Records

The Privacy Official shall maintain a written record of all actions, activities, designations, notices, consents and authorizations required under or taken in accordance with this Plan, the Privacy Policies and Procedures or the Privacy Regulations. Such records shall be maintained for a period of six (6) years from the date of creation or date when such records were last in effect, whichever is later.

SECTION 3: OVERVIEW OF THE SECURITY RULE

The Security Rule establishes minimum standards for the security of the storage and transmission of information that the Privacy Regulations set out to protect. The Security Rule became effective on April 21, 2005. Covered Entities, such as the ASC, and its Business Associates must comply with the Security Rule. The Security Rule applies only to information received, created, stored, maintained, or transmitted in any electronic media or format (the "ePHI"). Basically, the Privacy Regulations tell what should be protected and the Security Rule tells an entity how to protect it.

The Security Rule is intended to ensure the integrity, confidentiality and availability of ePHI. The Security Rule requires Covered Entities to implement safeguards to prevent improper access to ePHI that is stored in electronic form, including information contained in e-mails or other electronic transactions.

The Security Rule contains "standards" and "implementation specifications." Generally, a standard explains a requirement that must be accomplished and implementation specifications explain how to do it. The standards are categorized into three groups: administrative, physical, and technical, and collectively these groups are known as "safeguards." Implementation specifications are either required or addressable. An implementation specification is required if the Department of Health and Human Services ("HHS") believes that such specification is critical, and if so, the specification be implemented. When an implementation specification is considered addressable, it means that HHS believes that it is one that is not likely to be an issue with every covered entity, but must be addressed if one or more apply to a covered entity's

particular circumstances. Each ASC shall develop policies and procedures for all required implementation specifications. If each ASC believes that an addressable specification reasonably and appropriately applies to it, then the ASC shall implement such specification. If the ASC determines that the specification is simply not applicable then no action shall be taken. However, the ASC shall document the rationale for the specification not being applicable to it.

The Secretary of HHS is expected to issue guidance on the most effective and appropriate technical safeguards for use in carrying out the standards contained in the Security Rule by February 17, 2010 and annually thereafter. ASC shall comply with this guidance by its effective date to the extent such guidance is applicable to the activities of ASC. The ASC will issue notifications regarding the same to its employees, Members, officers and agents.

Covered Entities that do not comply with the Security Rule requirements are subject to a number of penalties. Civil penalties can range from $100.00 per violation, to $1,500,000 per person for instances of uncorrected willful neglect. Criminal penalties for Security Rule violations range from a $50,000.00 fine and one (1) year in prison up to a $250,000 fine and ten (10) years in prison.

SECTION 4: COMPLIANCE GUIDELINES

I. Security Official

Each ASC's Security Official shall be a qualified and trained Security Officer that shall report to the ASC's HIPAA Compliance Committee. The Security Official may be the same person as the Privacy Official. The Security Official at each ASC shall be responsible for:

1. developing, implementing and maintaining the ASC's Security Rule Policies and Procedures;

2. overseeing, monitoring and maintaining the ASC's Security Rule compliance activities;

3. training employees on Security Rule Policies; and

4. performing periodic assessments to determine any modifications needed for the ASC's Security Rule Policies and Procedures.

II. HIPPA Compliance Committee

The HIPAA Compliance Committee for each ASC (the formation is discussed in Section II of the Plan) shall be responsible for:

1. working with the Security Official to develop the ASC's Security Rule Policies and Procedures; and

2. recommending and monitoring, in conjunction with the Security Official, the development of internal systems and controls to carry out the Security Rule Policies and Procedures.

III. **Standards and Procedures**

Each ASC shall develop and implement written compliance policies and procedures (the "Security Rule Policies and Procedures") to comply with the Security Rule. Each ASC shall adhere to the following standards:

A. Risk Analysis

Before development of the Security Rule Policies and Procedures occurs, the ASC shall conduct a risk analysis and asset identification to determine the following:

(1) What systems process, store, retrieve or access ePHI?

(2) Does a database contain ePHI?

(3) Where did the ePHI come from and where is the ePHI going?

(4) Who has access to the ePHI?

(5) What security measures follow the ePHI?

The ASC shall then determine what vulnerabilities may exist and what security "gaps" need to be addressed by the ASC's Security Rule Policies and Procedures so that risk can be reduced to an acceptable level.

B. Standards and Implementation Specifications

The ASC shall develop written policies and procedures that conform to the standards and implementation specifications contained in the Security Rule. The following is a brief description of such standards and specifications that must be implemented and/or addressed by the ASC:

Administrative Safeguards:

1. Security Management: The ASC will develop policies and procedures that prevent, detect and correct security violations. Such policies shall include as follows:

(A) Risk Analysis (Mandatory): The ASC must conduct a thorough assessment of the potential risks and vulnerabilities to the security of ePHI.

(B) Risk Management (Mandatory): The ASC shall maintain security measurements sufficient to reduce risks and vulnerabilities to the Security of ePHI.

(C) Sanction Policy (Mandatory): The ASC shall have a written sanction policy for employees who commit Security Rule violations. Corrective

actions and sanctions should be graduated according to the severity of the breach.

(D) Information System Activity Review (Mandatory): The ASC shall continually review all policies to make sure they are effective. This includes reviews of audit logs, access reports, tracing failed password attempts, and security incident reports and trends.

2. Workforce Security: The ASC shall implement policies and procedures to ensure that all members of the work force who require access to ePHI are granted such access, and that access to ePHI is restricted from those members of the work force that do not require such access.

(A) Authorization and/or Supervision: The ASC shall "clear" each employee who is present in an area where access to ePHI is available and employees working with ePHI must be subject to progressive levels of supervision.

(B) Workforce Clearance Procedure: The ASC shall implement procedures to determine that access to ePHI by a particular individual is appropriate.

(C) Termination Procedure: The ASC shall have a policy in place for the termination of access to ePHI in the event that an employee is terminated or the employee changes positions within the ASC to a job that no longer requires access to ePHI.

3. Information Access Management: The ASC shall implement policies and procedures to authorize access to ePHI.

(A) Access Authorization: The ASC shall establish procedures to ensure that employees who are "cleared" are further "authorized" for access to ePHI.

(B) Access Establishment and Modification: The ASC shall implement a policy to monitor the workforce and their individual needs for access to ePHI, and establish procedures for the modification or revocation of such access.

4. Security Awareness and Training Program: The ASC shall implement a security awareness training program for all employees that addresses the following:

(A) Security Reminders (Mandatory): The ASC shall have a policy to regularly remind each ASC employee of the ASC's Security Rule Policies and Procedures.

(B) Protection from Malicious Software (Mandatory): The ASC shall have an anti-virus program.

(C) Log-In Monitoring (Mandatory): The ASC shall have a procedure to monitor log-on attempts.

(D) Password Management: The ASC shall establish procedures to manage the selection and periodic revision of access passwords.

5. Security Incident Procedures: The ASC shall have internal investigation procedures and procedures for responding to security incidents and for reporting the results of such response investigations.

6. Contingency Plan: The ASC shall implement a set of procedures in order to respond to any emergency or other occurrence that damages any system that contains ePHI.

(E) Data Backup Plan (Mandatory): The ASC shall have procedures for the creation and maintenance of retrievable exact copies of any original files lost.

(F) Disaster Recovery Plan: The ASC shall have a set of procedures on how to access covered entity's backup data.

(G) Emergency Mode Operation Plan (Mandatory): The ASC shall develop backup procedures concerning emergencies, when usual policies and procedures for the protection of ePHI cannot be utilized.

(H) Testing and Revision Procedure: The ASC shall develop a plan to periodically test their electronic security systems and to remedy any test failures.

(I) Applications and Data Criticality Analysis: The ASC shall review all ePHI access programs in use. Any data stored by such applications should be assessed to determine if a data set is critical to operations. The covered entity must implement a procedure to readily restore any critical data prior to the restoration of less critical data.

Physical Safeguards:

7. Facility Access Controls: The ASC shall have policies and procedures to assure those employees with authorization can access ePHI, while restricting access to those without necessary authorization.

(J) Contingency Operations (Mandatory): The ASC shall establish procedures to give authorized personnel physical access to all workstations or hardware containing ePHI, at all times that the ASC operates.

(K) Facility Security Plan (Mandatory): The ASC shall have policies and procedures to limit physical access to areas where ePHI can be accessed.

(L) Access Control and Validation Procedures: The ASC shall implement a means of controlling and validating an individual's access to facilities

where ePHI may be accessed, based on the individual's role or function. In other words, "minimum necessary" access.

(M) Maintenance Records: The ASC shall document the state of the physical ePHI security mechanisms in place, and the maintenance plan and actual damage, failures and repairs that have occurred to the physical mechanisms.

8. Workstation Use and Security: The ASC shall have designated workstations for accessing ePHI and shall protect the physical location of the workstations that access ePHI.

9. Device and Media Controls: The ASC shall implement procedures that govern the receipt and removal of hardware and electronic media that contains ePHI. Policies shall address the tracing of all incoming equipment where and to whom the equipment has been delivered, transfers of equipment between employees and ultimately the disposal of the devices.

(N) Disposal (Mandatory): The ASC shall implement procedures to assure that ePHI does not remain on discarded computers or components.

(O) Media Re-Use (Mandatory): The ASC shall have a procedure to "scrub" ePHI from non-volatile memory media when the media is to be reissued or decommissioned.

(P) Accountability: The ASC shall document and tract movements of any hardware or electronic media that contains or accesses ePHI. The documentation should also include the identity of the employee responsible for the movement.

(Q) Data Backup and Storage: The ASC shall implement procedures to make current and accurate backup copies of ePHI data.

Technical Safeguards:

10. Access Control: The ASC shall have a means of appropriately granting or denying access to ePHI. The ASC shall do the following to control access:

(R) Unique User Identification (Mandatory): The ASC shall implement a procedure so that each user has a unique log-in identification and password.

(S) Emergency Access Procedures (Mandatory): The ASC shall implement procedures so that ePHI can be accessed in an emergency.

(T) Automatic Log-Off: The ASC shall have procedures to implement automatic log-off on workstations that have access to ePHI.

(U) Encryption and Decryption: The ASC shall have a procedure to encrypt ePHI.

11. Audit Controls: The ASC implement hardware, software, or procedural mechanisms that record and examine the activity in computer systems that contain or access ePHI.

12. Integrity: The ASC shall implement policies and procedures to protect ePHI from improper alteration or destruction.

13. Person or Entity Authentication: The ASC must implement procedures to verify that a person or entity seeking access to ePHI is actually that person or entity.

14. Transmission Security: The ASC shall implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network, such as the internet.

SECTION 5: NATIONAL PROVIDER INDENTIFIER

HIPAA requires that all Covered Entities, including the ASCs, must use a National Provider Identifier (the "NPI") to identify such providers in all electronic HIPAA transactions as of May 23, 2007. Each of the ASCs shall apply to the Centers for Medicare and Medicaid Services (CMS) for its NPI and shall obtain such NPI by May 23, 2007.

EXHIBIT A

CONSENT TO THE USE AND DISCLOSURE OF HEALTH INFORMATION FOR TREATMENT, PAYMENT, OR HEALTHCARE OPERATIONS

I understand that as part of my healthcare, Melville Surgery Center creates and maintains health records describing my health history. I understand that the surgery center may use this information as:

1. a basis for planning my care and treatment;

2. a means of communication among many health professionals who contribute to my care;

3. a means by which third-party payors can verify that services billed were actually provided; and

4. a tool for routine health care operations such as assessing quality and reviewing the competence of health care professionals.

I hereby consent to the surgery center's use and disclosure of my individually identifiable health information for the purposes listed above and other purposes relating to my treatment, the payment of my health care, and other health care operations of the surgery center. In addition, I acknowledge that I received on the date indicated below a copy of the _____ Surgery Center Notice of Privacy Practices, which describes the obligations of the surgery center regarding its use and disclosure of my individually identifiable health information and my rights regarding this information. I also understand that the surgery center reserves the right to change its notice and practices. If the surgery center changes the notice, I can obtain a revised copy by asking the administrator of the surgery center. I understand that I have the right to request restrictions as to how my health information may be used or disclosed to carry out treatment, payment, or other healthcare operations and that the surgery center is not required to agree to the restrictions requested, except that effective February 17, 2010 the ASC must grant a request to restrict disclosure of my health information for payment or health care operations purposes if the disclosure is to a health plan and the health information relates solely to a health care item or service for which the ASC has been paid out of pocket by me in full. If the ASC does agree to any additional restrictions, the ASC must comply with such restrictions.

_____ I request the following restrictions to the use or disclosure of my health information.

_____

_____

Effective Date of Notice:_____

_____ Date:_____

Signature of patient or patient's representative

Created on 6/3/2009
\8023865.7

Printed name of patient's representative:_____
Relationship to patient:_____

EXHIBIT B

PATIENT AUTHORIZATION FOR

RELEASE OF HEALTH INFORMATION

YOU MAY REFUSE TO SIGN THIS AUTHORIZATION

I hereby authorize the use or disclosure of my individually identifiable health information as described below. I understand that this authorization is voluntary. I understand that if my health information is used or disclosed, the released information may no longer be protected by privacy regulations issued by the federal government.

Patient Name:_____ Social Security Number:_____

Persons authorized to make the use or disclosure of the information:

_____

_____

Persons authorized to receive the information:

_____

_____

Specific description of information (including date(s)):

_____

_____

_____

1. Melville Surgery Center must complete the following:

   a. What is the purpose of the use or disclosure? (If the patient does not wish to state the purpose, indicate "at the patient's request"):

      _____

      _____

   b. Will the surgery center receive financial or in-kind compensation in exchange for using or disclosing the health information described above? Yes_____ No_____

2. The patient or the patient's representative must read and initial the following statements:

   a. I understand that my health care and payment for my health care will not be affected if I do not sign this form. Initials:_____

   b. I understand that I may see and copy the information described on this form if I ask for it, and that the surgery center will give me a copy of this form after I sign it. Initials:_____

   c. I understand that this authorization will expire on ____/____/_____. Initials:_____

d. I understand that I may revoke this authorization at any time by notifying the surgery center in writing, but if I do revoke it, the revocation will not have any effect on any actions the surgery center took before it received the revocation. Initials:_____

_____ _____
Signature of patient or patient's representative Date

Printed name of patient's representative:_____
Relationship to patient:_____

EXHIBIT C

MELVILLE SURGERY CENTER, LLC

PATIENT NOTICE OF PRIVACY PRACTICES

EFFECTIVE DATE: May 20, 2009.

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE READ IT CAREFULLY.

I. YOUR RIGHTS REGARDING MEDICAL INFORMATION ABOUT YOU

Your health record is the physical property of Melville Surgery Center. The information contained in the record, however, belongs to you. You have the right to:

A. Request a restriction or limitation on the medical information we use or disclose about you for your treatment, payment or health care operations. For example, you may request that a particular procedure be kept confidential and not shared with other providers. You also have the right to request a limit on the medical information we disclose about you to someone who is involved in your care or the payment for your care, like a family member or friend or when we notify a family member, personal representative or other person responsible for your care to inform them of your location and general condition. We are not required to agree to your requested restrictions, except that effective February 17, 2010 we must grant a request to restrict disclosure of your health information for payment or health care operations purposes if the disclosure is to a health plan and the health information relates solely to a health care item or service which has been paid out of pocket by you in full. If we do agree to a restriction, we will comply with your request unless the information is needed to provide you emergency treatment.

B. Obtain a copy of this Notice by requesting one from the administrator of the surgery center.

C. Inspect and obtain a copy of your health care record, including, effective February 17, 2010, your electronic health record if applicable, by submitting a request in writing to the administrator of the surgery center.

D. Amend your healthcare record if you feel that medical information that we have about you is incorrect or incomplete by requesting, in writing, that an amendment be made. You must provide a reason that supports your request.

E. Obtain a report of all of the disclosures of your health information that we have made to the extent required by law.

F. Request that we communicate with you about your medical information in a certain way or at a certain location within reasonable limits.

G. Revoke your authorization to use and disclose medical information about you, except to the extent that we have already used or disclosed your medical information.

II. OUR RESPONSIBILITIES REGARDING YOUR MEDICAL INFORMATION

We are required by law to:

A. Maintain the privacy of your health information.

B. Provide you with this Notice, which describes our legal duties and privacy practices with respect to information we collect about you and a revised copy of the Notice if it is amended or otherwise changes.

C. Abide by the terms of this Notice.

D. Notify you if we are unable to agree to a requested restriction.

E. Accommodate reasonable requests that you have made to have us communicate your health information to you in a certain way or at a certain location.

F. Provide notification to you in the instance that we discover that a breach of your unsecured health information has occurred, effective on or around September 17, 2009.

WE RESERVE THE RIGHT TO CHANGE THIS NOTICE. We reserve the right to make the revised and changed notice effective for medical information that we already have about you, as well as any information we receive in the future. We will post a copy of the current notice in the surgery center. The notice will contain the effective date on the first page. Each time you register at the surgery center for health care services, we will offer you a copy of the current notice in effect.

III. HOW WE MAY USE AND DISCLOSE MEDICAL INFORMATION ABOUT YOU

Each time you visit us, a record of your visit is made. We may use or disclose the health information contained in this record to certain employees and staff members of the surgery center or certain persons or entities outside the surgery center in certain situations without first obtaining your authorization. The following categories describe the different ways that we may use and disclose your medical information. We must obtain your prior written authorization before using or disclosing your medical information in all other situations which are not listed below.

A. Treatment. We may use medical information about you to provide you with medical treatment and services. We may disclose medical information about you to doctors, nurses, technicians, or other surgery center personnel who are involved in taking care of you at the surgery center.

For example, information obtained by a nurse, physician, or other member of your health care team will be recorded in your medical record and used to determine the course of treatment that should work best for you. Your physician will document in your record his or her expectations of the members of your health team. Members of your health care team will then record the actions that they took and their observations. By reading your medical record, the physician will know how you are responding to treatment.

B. Payment. We may use and disclose medical information about you so that the treatment and services you receive at the surgery center may be billed to and payment may be collected from you, an insurance company, or third party.

For example, we may need to give your insurance company information about surgery you received at the surgery center so that the insurance company will pay us or reimburse you for the surgery.

C. Health Care Operations. We may use and disclose medical information about you for the operations of the surgery center.

For example, members of the medical staff, the risk manager or quality improvement manager, or members of the quality improvement team may use information in your health record to assess the care and outcomes in your case and others like it. This information will be used in a way to improve the quality and effectiveness of the healthcare and services that we provide.

D. Appointment Reminders. We may use and disclose medical information to contact you as a reminder that you have an appointment for treatment or medical care at the surgery center.

E. Treatment Alternatives. We may use and disclose medical information about you to contact you about or recommend possible treatment options or alternatives that may be of interest to you.

F. Health-Related Benefits and Services. We may use and disclose your medical information to inform you about health-related benefits or services that may be of interest to you.

G. Individuals Involved in Your Care or Payment for Your Care. We may release medical information about you to a friend or family member who is involved in your medical care or who helps pay for your care. We must inform you that we are going to use or disclose your information for this purpose and provide you with an opportunity to agree to, restrict or object to the disclosure or use.

H. Notification. We may use or disclose your medical information to notify or assist in notifying a family member, personal representative, or other person responsible for your care of your location and general condition. We must inform you that we are going to use or disclose your information for this purpose and provide you with an opportunity to agree to, restrict or object to the disclosure or use.

I. As Required by Law. We will disclose medical information about you when required to do so by federal, state or local law.

J. Avert Serious Threat to Health or Safety. We may use and disclose medical information about you when necessary to prevent a serious threat to your health or safety or the health or safety of the public or another person. The surgery center, however, will only disclose the information to someone able to help prevent the threat.

K. Organ and Tissue Donation. Consistent with applicable law, we may disclose health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs for the purpose of tissue donation and transplant.

L. Business Associates. Some of the services provided at the surgery center are provided by business associates. For example, we contract with certain laboratories to perform lab tests. When we contract for these services, we may disclose your health information to our business associates so that they can perform the job we have hired them to do. To protect your health information, we require our business associates to appropriately safeguard your information.

M. Workers' Compensation. We may release medical information about you to the extent authorized and to the extent necessary to comply with the laws relating to workers' compensation or other similar programs established by law.

N. Public Health Risks. As required by law, we may disclose your health information to public health or legal authorities charged with preventing or controlling disease, injury, or disability.

O. Health Oversight Activities. We may disclose medical information to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure and disciplinary action that are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.

P. Lawsuits and Disputes. If you are involved in a lawsuit or a dispute, we may disclose medical information about you in response to a court or administrative order. We may also disclose medical information about you in response to a subpoena, discovery request, or other lawful process by someone else involved in a dispute, but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested.

Q. Law Enforcement. We may disclose health information for law enforcement purposes as required by law or in response to a valid subpoena.

R. Coroners, Medical Examiners and Funeral Directors. We may release medical information to a coroner or medical examiner for purposes of identifying a deceased, determining a cause of death, or other duties authorized by law. We may also disclose health information to funeral directors consistent with applicable law to carry out their duties.

S. Food and Drug Administration. We may disclose to the FDA health information related to adverse events with respect to food, supplements, products and product defects, or post marketing surveillance information or to enable product recalls, repairs, or replacement.

T. Inmates. If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release medical information about you to the correctional institution or law enforcement official.

U. Victims of Abuse, Neglect or Domestic Violence. We may release medical information to a government authority if we reasonably believe that you are a victim of abuse, neglect or domestic violence, to the extent authorized or required by law. We must inform you or your personal representative that we have disclosed information for this purpose unless we believe that telling you or your personal representative would place you in risk of serious harm or otherwise not be in your best interest.

V. Child Abuse. We may release medical information to a government authority authorized by law to receive reports of child abuse or neglect.

IV. OTHER USES OF MEDICAL INFORMATION

Other uses and disclosures of medical information not covered by this Notice or the laws that apply to us will be made only upon a specific written authorization that you provide to us. If you provide us authorization to use or disclose medical information about you, you may revoke that authorization, in writing, at any time. If you revoke your authorization, we will no longer use or disclose medical information about you for the reasons covered by your written authorization. The revocation, however, will not have any effect on any action the surgery center took before it received the revocation.

V. QUESTIONS OR COMPLAINTS

If you have questions and would like additional information, you may contact **Rita Colantuoni,** Administrator, **631-293-9700,** at the surgery center.

If you believe your privacy rights have been violated, you can submit a written complaint describing the circumstances surrounding the violation to **Rita Colantuoni**, Administrator, **631-293-9700**, at the surgery center or to the Secretary of Health and Human Services in Washington, D.C. You will not be penalized for filing any complaint.

EXHIBIT D

BUSINESS ASSOCIATE AGREEMENT

THIS AGREEMENT (this " Business Associate Agreement") is made as of this _____ day of _____, _____, by and between Melville Surgery Center, a Limited Liability Company formed under the laws of the State of New York (the "ASC"), and _____ ("Business Associate").

W I T N E S S E T H

WHEREAS, the ASC operates a freestanding Medicare-certified outpatient surgery center at _____ **1895 Walt Whitman Road, Melville, NY 11747** and is a "covered entity," as that term is defined under the Health Insurance Portability and Accountability Act of 1996, as amended, which includes the Standards for the Privacy of Individually Identifiable Health Information (the "Privacy Rule"), the Standards for Electronic Transactions, and the Security Rule (45 C.F.R. Parts 160–64), and the Privacy provisions (Subtitle D) of the Health Information Technology for Economic and Clinical Health Act and its implementing regulations (the "HITECH Act")(collectively "HIPAA");

WHEREAS, the ASC is committed to complying with HIPAA;

WHEREAS, Business Associate is committed to complying with the portions of HIPAA that are applicable to Business Associate and its relationship with Covered Entity;

WHEREAS, Business Associate provides _____ **[description of services Business Associate provides]**;

WHEREAS, the ASC and Business Associate (the "Parties") have entered into an agreement dated _____, 20__ (the "Agreement") for the purpose of _____ **[describe agreement]**.

WHEREAS, in discharging its duties under the Agreement, the Business Associate will receive protected health information ("PHI"), as defined below, of patients of the ASC;

WHEREAS, the ASC and Business Associate are required under HIPAA to enter into an agreement with each other regarding the Business Associate's use and disclosure of PHI that complies with each of the requirements set forth in 45 C.F.R. 164.504(e), as amended;

NOW, THEREFORE, in consideration of the premises above, the Parties, intending to be legally bound, hereby agree to the following:

1. Definitions. Unless otherwise provided in this Agreement, capitalized terms shall have the same meaning as set forth under HIPAA.

(a) "Individual" means the person who is the subject of PHI, and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

(b) "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. part 160 and part 164, subparts A and E, and any regulations promulgated in connection therewith.

(c) "Required by Law" shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.103.

(d) "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

(e) "Security Rule" shall mean the administrative, technical and physical safeguards set forth in 45 C.F.R. Parts 160–64, in compliance with Social Security Act §1473(d) (42 U.S.C. §1320-21d), and any regulations promulgated in connection therewith.

(f) "PHI" shall have the same meaning as the term "protected health information" in 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of the ASC.

(g) "Designated Record Set" shall have the same meaning as the term "designated record set" in 45 C.F.R. § 164.501.

(i) "Breach" shall have the same meaning as the term "breach" in Public Law 111-5 Section 13400 (1).

2. Obligations and Activities of Business Associate. Except as otherwise limited in this Business Associate Agreement, Business Associate may use or disclose PHI of the patients of the ASC to perform functions, activities, or services for, or on behalf of, the ASC as specified in the Agreement, provided that such use or disclosure would not violate the minimum necessary policies and procedures of the ASC or the Business Associate's obligations under the Privacy Rule, including 45 C.F.R. § 164.504(e), as amended.

(a) Business Associate agrees not to use or further disclose PHI other than as permitted or required by this Business Associate Agreement, the Privacy Rule as amended, or as Required by Law.

(b) Business Associate acknowledges that it is statutorily required to comply with the Security Rule and agrees to develop, implement, maintain and use appropriate administrative, technical and physical safeguards, in compliance with the Security Rule, to preserve the integrity and confidentiality of and to prevent non-permitted or violating use or disclosure of PHI received for or from ASC. Business Associate will document and keep these safeguards current.

(c) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI in violation of this Business Associate Agreement.

(d) Business Associate agrees to promptly report to the ASC any use or disclosure of PHI not provided for by this Agreement or under HIPAA of which it becomes aware including any Breach of unsecured PHI. If Business Associate reports any such Breach to the ASC, the notice provided by the Business Associate must include the identity of the individual whose unsecured PHI has been, or is reasonably believed to have been accessed, acquired or disclosed during such breach, and any additional information required by HIPAA. Business Associate agrees to cooperate with ASC upon report of any such Breach so that ASC may provide the individual affected by such Breach with proper notice as required by HIPAA.

(e) Business Associate agrees to ensure that any agent (including a subcontractor) to whom it provides PHI received from the ASC, or created or received by Business Associate on behalf of ASC, agrees to the same restrictions and conditions that apply through this BA Agreement with respect to such information.

(f) Business Associate agrees to provide access, at the request of the ASC, and in the time and manner designated by the ASC, to PHI in a Designated Record Set to the ASC, or as directed by the ASC, to an Individual in order to meet the requirements under 45 C.F.R. § 164.524.

(g) Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that the ASC directs or agrees to pursuant to 45 C.F.R. § 164.526 at the request of the ASC or an Individual, and in the time and manner designated by the ASC.

(h) Business Associate agrees to make internal practices, books, and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from the ASC, or created or received by Business Associate on behalf of the ASC, available to the ASC, or to the Secretary, for purposes of the Secretary determining the ASC's compliance with the Privacy Rule.

(i) Business Associate agrees to document its disclosures of PHI and maintain a log of information related to such disclosures in accordance with the requirements of 45 C.F.R. 164.528, and Public Law 111-5 Section 13405 (c).

(j) Business Associate agrees to provide to the ASC or an Individual, in the time and manner designated by ASC or as Required by Law**,** information collected in accordance with Section 2(i) of this Business Associate Agreement, to permit the ASC to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528 and Public Law 111-5 Section 13405 (c).

3. Obligations of the ASC.

(a) The ASC shall notify Business Associate of any limitation(s) in its privacy practices of the ASC in accordance with 45 C.F.R. § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

(b) The ASC shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

(c) The ASC shall notify Business Associate of any restriction to the use or disclosure of PHI that the ASC has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

4. Term and Termination.

(a) Term. The term of this Business Associate Agreement (the "Term") shall be effective as of _____, 20__, and shall terminate when all of the PHI provided by the ASC to Business Associate, or created or received by Business Associate on behalf of the ASC, is destroyed or returned to the ASC, or if it is infeasible to return or destroy such PHI, protections are extended to such information, in accordance with the termination provisions in this Section 4.

(b) Termination for Cause. Upon the ASC's knowledge of a material breach by Business Associate, the ASC shall either:

(1) Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Business Associate Agreement and the Agreement if Business Associate does not cure the breach or end the violation within the time specified by the ASC;

(2) Immediately terminate this Business Associate Agreement and the Agreement if Business Associate has breached a material term of this Business Associate Agreement and cure is not possible; or

(3) If neither termination nor cure are possible, the ASC shall report the violation to the Secretary.

Upon the expiration of the Cure Period, or immediately if the breach is not capable of being cured, the non-breaching Party may terminate this Business Associate Agreement.

(c) Effect of Termination.

(1) Except as provided in paragraph (b) of this Section 4, upon termination of this Business Associate Agreement, for any reason, Business Associate shall return or destroy all PHI received from the ASC or created or received on behalf of the ASC. This provision shall extend and apply to PHI that is in the possession of subcontractors or agents of Business Associate that is received from, or created or received on behalf of the ASC. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI.

(2) In the event that Business Associate determines that returning or destroying the PHI is not feasible, Business Associate shall provide to the ASC notification of the conditions that make return or destruction not feasible. Upon notice to the ASC by Business

Associate that return or destruction of the PHI is not feasible, Business Associate shall extend the protections of this Business Associate Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

5. Amendment. The Parties agree to take such action as is necessary to amend this Business Associate Agreement from time to time as is necessary for the ASC to comply with the requirements of HIPAA and the Privacy Rule.

6. Survival. The respective rights and obligations of the Parties under Section 4 of this Business Associate Agreement shall survive the termination of the Term of this Business Associate Agreement.

7. Interpretation. Any ambiguity in this Business Associate Agreement shall be resolved in favor of a meaning that permits the ASC to comply with HIPAA.

8. Notice. Any and all communications required under this Business Associate Agreement shall be sent by registered or certified mail, return receipt requested, postage prepaid, and shall be addressed to the recipient's last known business address.

9. Counterparts. This Business Associate Agreement may be executed in two or more counterparts, each of which shall constitute an original but all of which together shall constitute one and the same instrument.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement as of the day herein first above written.

MELVILLE SURGERY CENTER	**[NAME OF BUSINESS ASSOCIATE]**
By:_____	By:_____
Its:_____	Its:_____