MAPPING GUIDE

Imprivata FairWarning capabilities mapping to HIPAA

The Health Insurance Portability and Accountability Act's (HIPAA) Privacy, Security, and Breach Notification Rules protect the privacy and security of health information and provide individuals with certain rights to their protected health information. The three HIPAA rules are:

- The **Privacy Rule**, which sets national standards for when protected health information (PHI) may be used and disclosed by covered entities and their business associates,
- The **Security Rule**, which specifies safeguards that covered entities and their business associates must implement to protect the confidentiality, integrity, and availability of electronic protected health information,
- The **Breach Notification Rule**, which requires covered entities to notify affected individuals; U.S. Department of Health & Human Services (HHS); and, in some cases, the media of a breach of unsecured PHI. Business associates are required to notify the covered entity of breaches at or by the business associate.

Imprivata FairWarning Patient Privacy Intelligence fully addresses 5 of the protocol elements and partially addresses 26 of the protocol elements. The Imprivata FairWarning solution assists customers in addressing key HIPAA requirements ranging from Security Management Process, Workforce Security, Security Awareness, Sanctions, Security Incident Procedures to many others. Many of the HIPAA requirements are problematic if not impossible to address without Imprivata FairWarning.
The HHS HIPAA information is available at https://www.hhs.gov/hipaa/for-professionals/index.html.

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.530(d)(2)	§164.530(d)(2) Implementation specification: Documentation of complaints. As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.	Complaints to the Covered Entity	Has the covered entity documented all complaints received and their disposition consistent with the performance criteria? Obtain and review a sample of documentation of complaints for consistency with the established performance criterion.	Imprivata FairWarning provides incident tracking and management via the Investigations section, allowing for full documentation of post-incident analyses, resolution, mitigation, and other activities, including patient complaints	Full	PPM
§164.530(e)(1)	§164.530(e)(1) Standard: Sanctions. A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart or subpart D of this part. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of § 164.502(j) or paragraph (g)(2) of this section.	Sanctions	Does the covered entity apply appropriate sanctions against members of the workforce who fail to comply with the privacy policies and procedures of the entity or the Privacy Rule? Obtain and review policies and procedures to determine if the entity has and applies sanctions consistent with the established performance criterion. Obtain and review documentation of the application of sanctions to a sample of workforce members to determine whether appropriate sanctions were applied. (Note: OCR is not looking for violations in order to take enforcement action; we are restricting our analysis to whether appropriate sanctions consistent with the entity policies have been applied.)	Imprivata FairWarning provides incident tracking and management via the Investigations section, allowing for full documentation of post-incident analyses, resolution, mitigation, and other activities, including any sanctions.	Partial – (we cannot apply the sanctions) We can only provide a repository for documenting the resolution of violations	IM/GR

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.530(f)	§164.530(f) Standard: Mitigation. A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.	Mitigation	Does the covered entity mitigate any harmful effect that is known to the covered entity of a use or disclosure of PHI by the covered entity or its business associate+A5:G50violation of its policies and procedures? Obtain and review policies and procedures in place for consistency with the established performance criterion. Determine whether a process is in place to ensure mitigation actions are taken pursuant to the policies and procedures. From a population of instances of non-compliance within the audit period, obtain and review documentation to determine whether mitigation plans were developed and applied pursuant to the policies and procedures. [Note: OCR is not looking for violations in order to take enforcement action; we are restricting our analysis to whether appropriate mitigation plans consistent with the entity policies have been developed and applied] Obtain and review documentation that the policies and procedures are conveyed to the workforce.	Imprivata FairWarning provides incident tracking and management via the Investigations section, allowing for full documentation of post-incident analyses, resolution, mitigation, and other activities, including any sanctions.	Partial – We can provide the documentation and tracking for mitigation.	PPM

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.530(b)	§164.530(b)(1) Standard: Training. A covered entity must train all members of its work- force on the policies and procedures with respect to protected health information required by this subpart and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.	Training	Does the covered entity train its work force and have a policies and procedures to ensure all members of the workforce receive necessary and appropriate training in a timely manner as provided for by the established performance criterion? Obtain and review such policies and procedures. Areas to review include training each new member of the workforce within a reasonable period of time and each member whose functions are affected by a material change in policies or procedures. From the population of new hires within the audit period, obtain and review a sample of documentation of necessary and appropriate training on the HIPAA Privacy Rule that has been provided and completed. Obtain and review documentation that workforce members have been trained on material changes to policies and procedures required by the HITECH Act.	MPS Provides training documentation along with a communication plan for customers to roll-out to their organization.	Partial (We cannot distinguish employees who receive training) MPS provides training and awareness materials that can be used with the customer's workforce.	MPS
§164.530(d)(1)	§164.530(d)(1) Standard: Complaints to the covered entity. A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart and subpart D of this part or its compliance with such policies and procedures or the requirements of this subpart or subpart D of this part.	Complaints to the Covered Entity	Does the covered entity have a process for individuals to make complaints, consistent with the requirements of the established performance criterion? Obtain and review policies and procedures to determine how complaints are received, processed, and documented.	MPS Reviews policies to verify if there is documentation for employees and patients to contact the privacy office for complaints.	Partial – MPS verifies customers have a point of contact for compliants.	MPS

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.530(e)(1)	§164.530(e)(1) Standard: Sanctions. A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart or subpart D of this part. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of § 164.502(j) or paragraph (g)(2) of this section.	Sanctions	Does the covered entity apply appropriate sanctions against members of the workforce who fail to comply with the privacy policies and procedures of the entity or the Privacy Rule? Obtain and review policies and procedures to determine if the entity has and applies sanctions consistent with the established performance criterion. Obtain and review documentation of the application of sanctions to a sample of workforce members to determine whether appropriate sanctions were applied. (Note: OCR is not looking for violations in order to take enforcement action; we are restricting our analysis to whether appropriate sanctions consistent with the entity policies have been applied.)	MPS Reviews policies to verify if documentation meets OCR requirements for appropriate sanctions to workforce members.	Partial	MPS/IM/GR

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.530(i)	§164.530(i)(1) Standard: Policies and procedures. A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart and subpart D of this part. The policies and procedures must be reasonably designed, taking into account the size and the type of activities that relate to protected health information undertaken by a covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart.	Policies and Procedures	Has the covered entity implemented policies and procedures with respect to PHI that are designed to comply with the standards, implementation specifications, and other requirements of the HIPAA Privacy Rule? Obtain and review documentation that, consistent with the established performance criterion address the following: • The policies and procedures are reasonably designed to ensure compliance for the size and type of activities performed. • The entity changes these policies and procedures as necessary to comply with changes in the law. • The entity documents and implements such changes promptly. • Any corresponding material changes are made to the notice of privacy practices. Obtain copies of policies and procedures in place in the previous calendar year and January 1, 2012, and the corresponding notices of privacy practices in effect on those dates. Determine whether material changes (e.g., for health plans, limits on use of genetic information for underwriting purposes; for health care providers, that a request for restriction must be accepted in certain situations) required by the HITECH omnibus rule are incorporated into the recent policies and procedures and are reflected in the notice of privacy practices.	MPS performs a policy review and as part of the policy review we look to ensure the policies are current and how often the policies are reviewed and/or updated.	Partial	MPS

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.530(d)	164.530(d)(1) Standard: Complaints to the covered entity. A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart and subpart D of this part or its compliance with such policies and procedures or the requirements of this subpart or subpart D of this part. (2) Implementation specification: Documentation of complaints. As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.	Complaints	Inquire of management as to whether formal or informal policies and procedures exist for receiving and processing complaints over the entity's privacy practices. Obtain and review formal or informal policies and procedures to determine how complaints are received, processed, and documented. From a population of complaints received within the audit period, obtain and review documentation of each complaint.	Imprivata FairWarning provides incident tracking and management via the Investigations section, allowing for full documentation of post-incident analyses, resolution, mitigation, and other activities, including patient complaints	Partial	IM/GR

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.530(e)	164.530(e)) Standard: Sanctions. A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart or subpart D of this part. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of § 164.502(j) or paragraph (g)(2) of this section.	Sanctions	Inquire of management as to whether sanctions are in place against members of the covered entity's workforce who fail to comply with the privacy policies and procedures. Obtain and review formal or informal policies and procedures to determine if sanctions are identified/described in the event members of the workforce do not comply with the entity's privacy practices. From a population of instances of individual/ employee non-compliance within the audit period, obtain and review documentation to determine whether appropriate sanctions were applied. Obtain and review evidence that the policies and procedures are updated and conveyed to the workforce.	Imprivata FairWarning provides incident tracking and management via the Investigations section, allowing for full documentation of post-incident analyses, resolution, mitigation, and other activities, including patient complaints	Partial	IM/GR

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.402	§164.402 (1)(i) For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual. (ii) A use or disclosure of protected health information that does not include the identifiers listed at § 164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.	Definitions: Breach – Risk Assessment	Does the covered entity have policies and procedures for determining whether an impermissible use or disclosure requires notifications under the Breach Notification Rule? Does the covered entity have a process for conducting a breach risk assessment when an impermissible use or disclosure of PHI is discovered, to determine whether there is a low probability that PHI has been compromised? If not, does the covered entity have a policy and procedure that requires notification without conducting a risk assessment for all or specific types of incidents that result in impermissible uses or disclosures of PHI? Obtain and review policies and procedures regarding the process for determining whether notifications must be provided when there is an impermissible acquisition, access, use, or disclosure of PHI. If the entity does not have a policy and procedure that treats all potential breaches as requiring notifications without conducting a risk assessment, review the covered entity's risk assessment policies and procedures. Evaluate whether they require the covered entity to consider at least the following four factors: (i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification (ii) The unauthorized person who used the PHI or to whom the disclosure was made (iii) Whether the PHI was actually acquired or vie (iv) The extent to which the risk to the PHI has been mitigated. Obtain a list of risk assessments, if any, conducted within the specified period where the covered entity determined there was a low probability of compromise to the PHI. Use sampling methodologies to select documentation of risk assessments to assess whether the risk assessments were completed in accordance with §164.402(2). Obtain a list of risk assessments, if any, conducted within the specified period where the covered entity determined that the PHI was compromised and notification were required under 164.404-164.408. Use sampling methodologies to select documentation of risk assessments to assess whether the risk assessments were completed in accordance with §164.402(2).	imprivata FairWarning provides incident tracking and management via the Investigations section, allowing for full documentation of post-incident analyses, resolution, mitigation, and other activities, including patient complaints. This includes a tool for performing a risk of compromise assessment.	Partial	IM

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.402	§164.402 - Definitions: Breach Exceptions - Unsecured PHI (2) Breach excludes: (i) Any unintentional acquisition, access, or use of protected health information by a work- force member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part. (ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.(iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5 on the HHS website.	Definitions: Breach - exceptions	Did the covered entity or business associate determine that an acquisition, access, use or disclosure of protected health information in violation of the Privacy Rule not require notifications under §§164.404-164.410 within the specified period? • If yes, did the covered entity or business associate determine that one of the regulatory exceptions to the definition of breach at §164.402(1) apply? If yes, obtain documentation of such determination. Use sampling methodologies to select and review documentation that such were completed in accordance with §164.402. • If yes, did the covered entity or business associate determine that the breach did not require notification, under §§164.404-410, because the PHI was not unsecured PHI, i.e., it was rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified in the applicable guidance? If yes, obtain and review documentation. Use sampling methodologies to select and review documentation that such were completed in accordance with §164.402.	FairWarning provides incident tracking and management via the Investigations section, allowing for full documentation of post-incident analyses, resolution, mitigation, and other activities, including patient complaints. This includes a tool for performing a risk of compromise assessment.	Full	IM

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.404(a)	§164.404(a)(1) General rule. A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured deemed breaches and will allow you to protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.	Notice to individuals	Does the covered entity have policies and procedures for notifying individuals of a breach of their protected health information. Obtain and review a list of breaches, if any, in the specified period involving 500 or more individuals. Obtain and review documentation of notifications provided to the affected individuals consistent with the requirements in §164.404(a)(1).	Imprivata FairWarning provides governance reports that will identify incidents through the investigation module that have been deemed breaches and will allow you to report on those under 500 as well as those over 500.	Partial	IM/GR
§164.404(b)	§164.404(b)) Implementation specification: Timeliness of notification. Except as provided in § 164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.	Timeliness of notification	Were individuals notified of breaches within the required time period? Inquire of management. Obtain and review the policies and procedures for notifying individuals of breaches and determine whether such policies and procedures are consistent with §164.404, including providing notification without unreasonable delay and in no case later than within 60 days of discovery of a breach. Obtain and review a list of breaches, if any, in the specified period and documentation indicating the date individuals were notified, the date the covered entity discovered the breach, and the reason, if any, for delay in notification to determine whether all individuals were notified consistent with §164.404(a), (b).	Imprivata FairWarning provides governance reports that will identify incidents through the investigation module that have been deemed breaches and allow you to track individual notifications.	Partial	IM/GR

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.406	§164.406(a) Standard. For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach as provided in § 164.404(a)(2), notify prominent media outlets serving the State or jurisdiction. For purposes of this section, State includes American Samoa and the Northern Mariana Islands.	Notification to the media	Does the covered entity have policies and procedures for notifying media outlets of breaches affecting more than 500 residents of a State or jurisdiction? Obtain and review policies and procedures. Evaluate whether the specifications at §164.406 are met. Obtain and review a list of breaches, if any, in the specified period affecting more than 500 residents of a State or jurisdiction. Obtain and review documentation to verify that the media notifications included the elements required by §164.406.	Imprivata FairWarning provides governance reports that will identify incidents through the investigation module that have been deemed breaches and will allow you to report on those under 500 as well as those over 500 and if they have been reported to the Secretary as required.	Partial	IM/GR

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.408	§164.408 (a) Standard. A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in § 164.404(a)(2), notify the Secretary. (b) Implementation specifications: Breaches involving 500 or more individuals. For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, except as provided in § 164.412, provide the notification required by paragraph (a) of this section contemporaneously with the notice required by § 164.404(a) and in the manner specified on the HHS website. (c) Implementation specifications: Breaches involving less than 500 individuals. For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches occurring during the preceding calendar year, in the manner specified on the HHS website.	Notification to the Secretary	Does the covered entity have policies and procedures for notifying the Secretary of breaches involving 500 or more individuals? Does the covered entity have policies and procedures for notifying the Secretary of breaches involving less than 500 individuals? Obtain and review policies and procedures. Evaluate whether the specifications at §164.408 are met. Obtain and review a list of breaches, if any, in the specified period involving 500 or more individuals. Obtain and review documentation of notifications provided to the Secretary. Determine whether contemporaneous notifications were provided to the Secretary consistent with the requirement in §164.408. Use sampling methodologies to select notifications to be reviewed and verify that the notices include the elements required by §164.408. Obtain and review a list of breaches, if any, in the specified period involving fewer than 500 individuals. Obtain and review documentation of notifications provided to the Secretary . Evaluate whether the notifications were provided to the Secretary within 60 calendar days of the end of the calendar year in which the breach was discovered, consistent with the requirement in §164.408. Use sampling methodologies to select notifications to be reviewed and verify that the notices include the elements required by §164.408.	Imprivata FairWarning provides governance reports that will identify incidents through the investigation module that have been deemed breaches and will allow you to report on those under 500 as well as those over 500 and if they have been reported to the Secretary as required.	Partial	IM/GR

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.414(b)	§164.414(b) Burden of proof. In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosure did not constitute a breach, as defined at § 164.402.	Burden of Proof	Inquire of management as to whether a risk assessment process exists to determine significant harm in a breach. Inquire of management as to whether a process exists to ensure that all notifications were made as required or that the impermissible use or disclosure did not constitute a breach. Obtain and review documentation of uses or disclosures that were not determined to be breaches and the corresponding risk assessment documentation.	Imprivata FairWarning provides incident tracking and management via the Investigations section, allowing for full documentation of post-incident analyses, resolution, mitigation, and other activities, including patient complaints. This includes a tool for performing a risk of compromise assessment.	Full	
§164.530(e)	164.530(e)) Standard: Sanctions. A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart or subpart D of this part. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of § 164.502(j) or paragraph (g)(2) of this section.	Sanctions	Does the covered entity apply appropriate sanctions against members of the workforce who fail to comply with the privacy policies and procedures of the entity or the Privacy Rule?	MPS Reviews policies to verify if documentation meets OCR requirements for appropriate sanctions to workforce members, however we cannot confirm the covered entity applies sanctions I accordance with their policy.	Partial	MPS

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.306(a)	§164.306(a): Covered entities and business associates must do the following:	General Requirements	General requirements, not a part of an audit inquiry: The Security Rule compliance practices of covered entities and business associates will be audited against the specific requirements described in the following sections. These specific requirements will be assessed based on the overarching principles set forth in the general requirements that pertain to all the security standards. Specifically, does the covered entity or business associate: 1. Ensure confidentiality, integrity and availability of ePHI? 2. Protect against reasonably anticipated threats or hazards to the security or integrity of ePHI? 3. Protect against reasonably anticipated uses or disclosures of ePHI that are not permitted or required by the Privacy Rule? 4. Ensure compliance with Security Rule by its workforce?	Imprivata FairWarning Analytics record and examine activity in systems with ePHI. These Analytics are then automated as Enforced Policies to proactively alert users of any activity that is being tracked or audited. Imprivata FairWarning assists customers in addressing one of the most common risk areas identified during a risk assessment, insider misuse of access to electronic health records. Imprivata FairWarning has many materials available to help you make the best use of patient privacy monitoring, and therefore reduce your risk.	Partial – FairWarning is a component of a well rounded comprehensive security program.	PPM

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.308(a)	§164.308(a): A covered entity or business associate must in accordance with 164.306:	Security Management Process	Does the entity have written policies and procedures in place to prevent, detect, contain and correct security violations? Does the entity have written policies and procedures in place to prevent, detect, contain and correct security violations? Does the entity prevent, detect, contain and correction security violations? Obtain and review policies and procedures related to security violations. Evaluate the content relative to the specified performance criteria for countermeasures or safeguards implemented to prevent, detect, contain and correct security violations. Obtain and review documentation demonstrating that policies and procedures have been implemented to prevent, detect, contain, correct security violations. Evaluate and determine if the process used is in accordance with related policies and procedures. Obtain and review documentation of security violations and remediation actions. Evaluate and determine if security violations where handled in accordance with the related policies and procedures; safeguards or countermeasures to prevent violations from occurring; identify and characterize violations as they happen; limit the extent of any damages caused by violations; have corrective action plan in place to manage risk.	Imprivata FairWarning application detects potential security violations. Imprivata FairWarning provides incident tracking and management via the Investigations section, allowing for full documentation of post-incident analyses, resolution, mitigation, and other activities, including patient complaints	Partial	PPM

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.308(a)(1)(ii)(B)	§164.308(a)(1)(ii)(B): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).	Security Management Process – Risk Management	Does the entity have policies and procedures in place regarding a risk management process sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level? Does the entity have policies and procedures in place regarding a risk management process sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level? Has the entity implemented security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level? Obtain and review policies and procedure related to risk management. Evaluate and determine if the documents identify how risk will be managed, what is considered an acceptable level of risk based on management approval, the frequency of reviewing ongoing risks, and identify workforce members' roles in the risk management process. Obtain and review documentation demonstrating the security measures implemented and/or in the process of being implemented as a result of the risk analysis or assessment. Evaluate and determine whether the implemented security measures appropriately respond to the threats and vulnerabilities identified in the risk analysis according to the risk rating and that such security measures are sufficient to mitigate or remediate identified risks to an acceptable level.	Imprivata FairWarning assists customers in addressing one of the most common risk areas identified during a risk assessment, insider misuse of access to electronic health records. Imprivata FairWarning has many materials available to help you make the best use of patient privacy monitoring, and therefore reduce your risk.	Partial	PPM

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.308(a)(1)(ii)(C)	§164.308(a)(1)(ii)(C): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	Security Management Process – Sanction Policy	Does the entity have policies and procedures in place regarding sanctions to apply to workforce members who fail to comply with the entity's security policies and procedures? Does the entity apply appropriate sanctions against workforce members who fail to comply with its security policies and procedures? Obtain and review documentation of the sanction policies and procedures (which could be an aspect of a larger code of conduct). Evaluate if they contain a reasonable and appropriate process to sanction workforce members for failures to comply with the entity's security policies and procedures. Elements to review may include but are not limited to: • Personnel involved in the sanction process • Required steps and time period • Notification steps • Reason for the sanction • Identification of the sanctions applied to compliance failures • Documentation of the sanction outcome Obtain and review documentation demonstrating sanctions against work- force members. Evaluate and determine whether appropriate sanctions were applied for workforce members that failed to comply with security policies and procedures.	MPS Reviews policies to meet OCR standards. Imprivata FairWarning application allows users to monitor/track all sanctions performed	Partial	IM/GR

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.308(a)(1)(ii)(D)	§164.308(a)(1)(ii)(D): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Security Management Process – Information System Activity Review	Does the entity have policies and procedures in place regarding the regular review of information system activity? Does the entity regularly review records of information system activity? Obtain and review policies and procedures related to reviewing records of information system activities. Evaluate and determine if reasonable and appropriate processes are in place to review records of information system activities, such as audit logs, access reports, and security incident tracking reports. Elements to review may include but are not limited to: • How often a review is performed • How reviews are documented • Workforce members' roles and responsibilities in the regular records of the information systems activities • Types of activities which may require further investigation Obtain and review documentation demonstrating the records of information system activities that were reviewed such as audit logs, access reports, and security incident tracking reports. Evaluate and determine if information system records were reviewed in a timely manner and that the review was conducted and certified by appropriate personnel. Obtain and review documentation demonstrating the capabilities of the information system activity logs. Evaluate and determine whether key information systems have the capabilities to generate activity records; and, if so, are the capabilities turned on and records generated.	Imprivata FairWarning Analytics and Reports enable reviewing of information system activity such as audit logs and access reports. Imprivata FairWarning Investigations centralize management and tracking of security incidents.	Partial	PPM

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.308(a)(3)(i)	§164.308(a)(3)(i): Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	Workforce Security	Does the entity have policies and procedures in place to ensure all members of its workforce have appropriate access to ePHI? Does the entity ensure all members of its workforce have appropriate access to ePHI? Obtain and review the policies and procedures that ensure all members of its workforce only have access to ePHI that is required for each work- force member to do his or her job. Elements to review may include but are not limited to: • That different levels of access to information systems are appropriately approved and communicated • Ensuring that the workforce operates at privilege levels no higher than necessary to accomplish required job duties Obtain and review documentation demonstrating access granted to work- force members and their job descriptions. Evaluate and determine that access granted to workforce members correlate with their job functions/duties. Obtain and review documentation demonstrating that management reviews workforce members' access to information systems that contain ePHI to determine if access is appropriate. Evaluate and determine if workforce members' access to information systems that contain ePHI is certified and approved by appropriate management.	Imprivata FairWarning can be used to verify that the user actually has the role and access assigned.	Partial	PPM/II

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.308(a)(3)(ii)(C)	§164.308(a)(3)(ii)(C): Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(b).	Workforce security – Establish Termination Procedures	Does the entity have policies and procedures in place for terminating access to ePHI when employment or other arrangements with the workforce member ends? Does the entity have policies and procedures in place for terminating access to ePHI when employment or other arrangements with the workforce member ends? Does the entity terminate access to ePHI when employment or other arrangements with the workforce member ends? Obtain and review policies and procedures for terminating access to ePHI when the employment of, or other arrangement with, a workforce member's employment is terminated or job description changes to require more or less access to ePHI. Evaluate the content in relation to the specified performance criteria. Elements to review may include but are not limited to: • Recovery of access control devices and deactivation of information system access upon termination of employment, including voluntary termination and involuntary termination • Termination of access by an independent contractor or other business associate, if applicable • Appropriate changes in access levels and/or privileges pursuant to job description changes that necessitate more or less access to ePHI • Time frames to terminate access to ePHI • Exit interviews that include a discussion of privacy and security topics regarding ePHI Obtain and review documentation demonstrating that workforce members' access to ePHI was terminated. Evaluate and determine whether access to ePHI was terminated in a timely manner and consistent with related policies and procedures. Obtain and review documentation demonstrating changes in access levels for workforce members with ePHI access. Obtain and review documentation of the job duties of workforce members before and after ePHI access level was changed. Evaluate and determine whether access levels were changed appropriately and in accordance with workforce member job duties. Has the entity chosen to implement an alternative measure? If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	Imprivata FairWarning can be used to monitor that accounts are not used after termination	Partial	PPM/II

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.308(a)(5)(i)	§164.308(a)(5)(i): Implement a security awareness and training program for all members of its workforce (including management).	Security Awareness and Training	Does the entity have policies and procedures in place regarding a security awareness and training program? Does the entity provide security awareness and training to all new and existing members of its workforce? Obtain and review policies and procedures for security awareness and training program. Elements to review may include but are not limited to: • How workforce members are provided the security awareness and training • Identifies workforce members (including managers, senior executives, and as appropriate, business associates, and contractors) who will be provided with the security and awareness training • How workforce members will be provided with security and awareness training when there is a change in the entity's information systems • How frequently security awareness and training will be provided to all workforce members Obtain and review documentation demonstrating the implementation of a security awareness and training program including related training materials. Evaluate and determine whether the training program is reasonable and appropriate for workforce members to carry out their functions. Obtain and review documentation demonstrating that the security awareness and training programs are provided to the entire organization and made avail- able to independent contractors and business associates, if appropriate.	Imprivata FairWarning offers an assortment of materials, such as posters and brochures, designed to help educate your staff regarding access policies, and acceptable use of electronic health records, as well as your use of the Fair- Warning patient privacy intelligence platform to ensure appropriate access. These materials can be customized with your organization's name, logo and other specifics.	Partial	Marketing

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.308(a)(6)(ii)	§164.308(a)(6)(ii): Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	Security Incident Procedures – Response and Reporting	Does the entity have policies and procedures in place for identifying, responding to, reporting, and mitigating security incidents? Does the entity identify, respond to, report, and mitigate security incidents? Obtain and review policies and procedures related to responding and reporting security incidents. Evaluate and determine if incident response procedures are in place. Elements to review may include but are not limited to: • A methodology for defining security incidents based on levels of criticality • Provisions for reporting and responding to all types of known and suspicious security incidents based on criticality levels of such incidents • The roles and responsibilities of workforce members including the entity's security incident response team Obtain and review documentation of responding to, reporting, and mitigating security incidents. Evaluate and determine if security incident response, reporting, and mitigation procedures are followed by workforce members; are conducted in a timely manner; and their outcomes are properly documented and communicated to the appropriate work- force members.	Imprivata FairWarning provides incident tracking and management via the Investigations section, allowing for full documentation of post-incident analyses, resolution, mitigation, and other activities, including patient complaints	Partial	PPM

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.312(a)(1)	§164.312(a)(1): Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	Access Control	Has the entity implemented technical policies and procedure for the electronic information systems that maintain ePHI to allow access only to authorized users? Does the entity only allow access to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4) to electronic information systems that maintain electronic protected health information? Obtain and review policies and procedures related to access control. Evaluate the content relative to the specified performance criteria to determine if ePHI is only accessible to authorized persons or software programs. Elements to review may include but are not limited to: • Identification of the capabilities of electronic information system access controls (i.e., read-only, modify, full access) • Identification of the type of access controls implemented for the electronic information systems • Identification of how system and generic IDs/ accounts are implemented, managed and controlled by technical access controls • Workforce members' roles and responsibilities regarding the capabilities to add, modify, or delete user access • The frequency of review and verification of user access to electronic information systems that maintain ePHI • The frequency of review and verification of software program access to electronic information systems that maintain ePHI • How is removed upon termination or modified upon change of position Obtain and review documentation demonstrating the implementation of access controls for electronic information systems that maintain ePHI. Evaluate and determine if the electronic information systems have the capacity to enable access controls; if access controls can be enabled, are the enabled access controls configured in accordance with the access control policies and procedures; and how are the electronic information systems' technical access capabilities defined (i.e., read-only, modify, full-access).	Imprivata FairWarning could be used to verify that the user actually have the role and access assigned.	Partial	PPM/II

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.312(a)(1) continued	§164.312(a)(1): Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	Access Control	Obtain and review documentation demonstrating a list of new workforce members from the electronic information system who was granted access to ePHI. Obtain and review documentation demonstrating the access levels granted to new workforce members. Evaluate and determine whether workforce members' access was approved; review the new workforce members' technical access granted and compare it to approved user access to determine that technical access is approved and granted in accordance with the access authorization requirements. Obtain and review documentation of a list of users with privileged access. Evaluate and determine whether the privileged access is appropriate based on the access control policies. Obtain and review a list of default, generic/shared, and service accounts from the electronic information systems with access to ePHI. Obtain and review documentation demonstrating the access levels granted to default, generic/shared, and service accounts. Evaluate and determine if the default, generic/shared, and service accounts are in use and that access has been approved and granted in accordance with the access authorization requirements. Obtain and review documentation demonstrating that periodic reviews of procedures related to access controls have been conducted. Evaluate and determine whether reviews have been performed of user access levels and evaluate the content in relation to the specified performance criteria. Obtain and review documentation demonstrating a list of terminations and job transfers. Obtain documentation demonstrating the removal or modification of user access levels. Evaluate and determine whether user access level removal or modification was approved and performed in accordance with the related policies and procedures.	Imprivata FairWarning could be used to verify that the user actually have the role and access assigned.	Partial	PPM/II

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.312(a)(2)(i)	§164.312(a)(2)(i): Assign a unique name and/or number for identifying and tracking user identity.	Access Control -- Unique User Identification	Does the entity have polices and procedures regarding the assignment of unique user IDs to track user identity? Does the entity assign unique user IDs to track user identity? Obtain and review policies and procedures regarding the assignment of unique user IDs. Evaluate the content of the policies and procedures in relation to the specified performance criteria to determine how user IDs are to be established and assigned. Obtain and review documentation demonstrating the assignment, creation, and use of unique user IDs in electronic information systems for user. Evaluate and determine if users are assigned a unique ID in accordance with the entity's policies and procedures for attributing new user IDs.	Imprivata FairWarning could be used to verify that the user have a unique ID in systems that contain ePHI.	Partial	PPM/II
§164.312(b)	§164.312(b): Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Audit Controls	Does the entity have policies and procedures in place to implement hard- ware, software and/or procedural mechanisms to record and examine activity in information systems that contain or use ePHI? Does the entity have hardware, software and/or procedural mechanism to record and examine activity in information systems that contain or use ePHI? Obtain and review documentation relative to audit controls. Evaluate whether risk-based audit controls have been implemented over all electronic information systems that contain or use ePHI. Elements to review may include but are not limited to: • Identification of the risk-based audit controls over all information systems that contain or use ePHI • How are systems and applications evaluated to determine if auditing controls should be implemented • Identification of what applications and systems will be audited • Procedures on how systems will be audited Obtain and review documentation demonstrating the implementation of hardware, software and/or procedural mechanisms to record and examine activity. Evaluate and determine whether information systems that contain or use ePHI activities are being recorded and examined; activities being recorded and examined appropriately and in accordance with related policies and procedures.	Imprivata FairWarning Analytics record and examine activity in systems with ePHI. These Analytics are then automated as Enforced Policies to proactively alert users of any activity that is being tracked or audited.	Full	MPS and PPM

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.308(a)	§164.308(a): A covered entity or business associate must in accordance with 164.306:	Security Management Process	Does the entity have written policies and procedures in place to prevent, detect, contain and correct security violations? Does the entity have written policies and procedures in place to prevent, detect, contain and correct security violations? Does the entity prevent, detect, contain and correction security violations? Obtain and review policies and procedures related to security violations. Evaluate the content relative to the specified performance criteria for countermeasures or safeguards implemented to prevent, detect, contain and correct security violations. Obtain and review documentation demonstrating that policies and procedures have been implemented to prevent, detect, contain, correct security violations. Evaluate and determine if the process used is in accordance with related policies and procedures. Obtain and review documentation of security violations and remediation actions. Evaluate and determine if security violations where handled in accordance with the related policies and procedures; safeguards or countermeasures to prevent violations from occurring; identify and characterize violations as they happen; limit the extent of any damages caused by violations; have corrective action plan in place to manage risk.	MPS Reviews policies and procedures surrounding monitoring and surveillance of workforce members using the organization's information systems	Partial	MPS

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.308(a)(1)(ii)(C)	§164.308(a)(1)(ii)(C): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	Security Management Process – Sanction Policy	Does the entity have policies and procedures in place regarding sanctions to apply to workforce members who fail to comply with the entity's security policies and procedures? Does the entity apply appropriate sanctions against workforce members who fail to comply with its security policies and procedures? Obtain and review documentation of the sanction policies and procedures (which could be an aspect of a larger code of conduct). Evaluate if they contain a reasonable and appropriate process to sanction workforce members for failures to comply with the entity's security policies and procedures. Elements to review may include but are not limited to: • Personnel involved in the sanction process • Required steps and time period • Notification steps • Reason for the sanction • Identification of the sanctions applied to compliance failures • Documentation of the sanction outcome Obtain and review documentation demonstrating sanctions against work- force members. Evaluate and determine whether appropriate sanctions were applied for workforce members that failed to comply with security policies and procedures.	MPS Reviews policies to meet OCR standards. Imprivata FairWarning application allows users to monitor/track all sanctions performed	Full	MPS

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.308(a)(1)(ii)(D)	§164.308(a)(1)(ii)(D): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Security Management Process – Information System Activity Review	Does the entity have policies and procedures in place regarding the regular review of information system activity? Does the entity regularly review records of information system activity? Obtain and review policies and procedures related to reviewing records of information system activities. Evaluate and determine if reasonable and appropriate processes are in place to review records of information system activities, such as audit logs, access reports, and security incident tracking reports. Elements to review may include but are not limited to: • How often a review is performed • How reviews are documented • Workforce members' roles and responsibilities in the regular records of the information systems activities • Types of activities which may require further investigation Obtain and review documentation demonstrating the records of information system activities that were reviewed such as audit logs, access reports, and security incident tracking reports. Evaluate and determine if information system records were reviewed in a timely manner and that the review was conducted and certified by appropriate personnel. Obtain and review documentation demonstrating the capabilities of the information system activity logs. Evaluate and determine whether key information systems have the capabilities to generate activity records; and, if so, are the capabilities turned on and records generated.	MPS Reviews policies and procedures surrounding monitoring and surveillance of workforce members using the organization's information systems	Partial	MPS

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.308(a)(3)(i)	§164.308(a)(3)(i): Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	Workforce Security	Does the entity have policies and procedures in place to ensure all members of its workforce have appropriate access to ePHI? Does the entity ensure all members of its workforce have appropriate access to ePHI? Obtain and review the policies and procedures that ensure all members of its workforce only have access to ePHI that is required for each work- force member to do his or her job. Elements to review may include but are not limited to: • That different levels of access to information systems are appropriately approved and communicated • Ensuring that the workforce operates at privilege levels no higher than necessary to accomplish required job duties Obtain and review documentation demonstrating access granted to work- force members and their job descriptions. Evaluate and determine that access granted to workforce members correlate with their job functions/ duties. Obtain and review documentation demonstrating that management reviews workforce members' access to information systems that contain ePHI to determine if access is appropriate. Evaluate and determine if workforce members' access to information systems that contain ePHI is certified and approved by appropriate management.	MPS Reviews policies and procedures surrounding role-based access and account authorization for information systems.	Partial	MPS

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.308(a)(3)(ii)(C)	§164.308(a)(3)(ii)(C): Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(b).	Workforce security – Establish Termination Procedures	Does the entity have policies and procedures in place for terminating access to ePHI when employment or other arrangements with the workforce member ends? Does the entity terminate access to ePHI when employment or other arrangements with the workforce member ends? Obtain and review policies and procedures for terminating access to ePHI when the employment of, or other arrangement with, a workforce member's employment is terminated or job description changes to require more or less access to ePHI. Evaluate the content in relation to the specified performance criteria. Elements to review may include but are not limited to: • Recovery of access control devices and deactivation of information system access upon termination of employment, including voluntary termination and involuntary termination • Termination of access by an independent contractor or other business associate, if applicable • Appropriate changes in access levels and/or privileges pursuant to job description changes that necessitate more or less access to ePHI • Time frames to terminate access to ePHI • Exit interviews that include a discussion of privacy and security topics regarding ePHI Obtain and review documentation demonstrating that workforce members' access to ePHI was terminated. Evaluate and determine whether access to ePHI was terminated in a timely manner and consistent with related policies and procedures. Obtain and review documentation demonstrating changes in access levels for workforce members with ePHI access. Obtain and review documentation of the job duties of workforce members before and after ePHI access level was changed. Evaluate and determine whether access levels were changed appropriately and in accordance with workforce member job duties. Has the entity chosen to implement an alternative measure? If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	MPS Reviews policies and procedures surrounding termination of access to information systems	Partial	

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.308(a)(4)(i)	§164.308(a)(4)(i): Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.	Information Access Management	Does the entity have policies and procedures in place for authorizing access to ePHI that supports the applicable requirements of the Privacy Rule? Does the entity authorize access to ePHI that supports the applicable requirements of the Privacy Rule? Obtain and review the policies and procedures to determine that they reasonably and appropriately restrict access to only those persons and entities with a need for access. Also obtain entity's policies and procedures related to minimum necessary [45 CFR 164.502(b)] and safeguards [45 CFR 164.514(d)] to determine that the policies and procedures subject to this inquiry support an entity's compliance with the minimum necessary requirement and safeguards requirement that limit unnecessary or inappropriate access to and disclosure of protected health information. Evaluate and determine whether the technical implementation of the access controls used by the entity support the minimum necessary policies and procedures and are consistent with the Privacy Rule safeguard policies.	MPS reviews role-based access and account authorization policies as well as minimum necessary policies.	Partial	MPS

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.308(a)(4)(ii)(B)	§164.308(a)(4)(ii)(B): Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	Information Access Management – Access Authorization	Does the entity have policies and procedures in place to grant access to ePHI for workforce members? Does the entity grant access to ePHI for workforce members? Obtain and review policies and procedures. Evaluate the content relative to the specified performance criteria for granting access, including whether authority to grant access and the process for granting access has been incorporated. Elements to review may include but are not limited to: • Workforce members or roles required to approve request to create information system accounts • Procedures to create enable, modify, disable, and remove information system accounts • Determination of what the authorization of access is based on Obtain and review documentation associated with granting of access to ePHI (i.e., paper or electronic request). Evaluate and determine if the procedures for granting access to ePHI are in accordance with related policies and procedures. Obtain and review documentation of newly hired workforce members' access to ePHI. Evaluate documentation to determine the granting of access to ePHI, including whether the levels of access they have to systems containing, transmitting, or processing ePHI, are appropriate. Has the entity chosen to implement an alternative measure? If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	MPS reviews role-based access and account authorization policies and acceptable use policies	Partial	MPS

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.308(a)(4)(ii)(C)	§164.308(a)(4)(ii)(C): Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	Information Access Management – Access Establishment and Modification	Does the entity have policies and procedures in place to authorize access and document, review, and modify a user's right of access to a workstation, transaction, program, or process? Does the entity authorize access and document, review, and modify a user's right of access to a workstation, transaction, program, or process? Obtain and review the policies and procedures. Evaluate their content relative to the specified performance criteria for authorizing access, and for documenting, reviewing, and modifying a user's right of access to a workstation, transaction, program, or process. Obtain and review documentation regarding individuals whose access to information systems has been reviewed based on access authorization policies. Evaluate and determine whether individuals' access has been reviewed and re-certified in a timely manner by the appropriate personnel. Obtain and review documentation demonstrating individuals whose access to information systems has been modified based on access authorization policies. Evaluate and determine whether modification of access to information systems is acceptable and modification of individuals' access to information systems was completed and approved by appropriate personnel. Has the entity chosen to implement an alternative measure? If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	MPS reviews role-based access and account authorization policies as well as acceptable use policies.	Partial	MPS

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.308(a)(5)(i)	§164.308(a)(5)(i): Implement a security awareness and training program for all members of its workforce (including management).	Security Awareness and Training	Does the entity have policies and procedures in place regarding a security awareness and training program? Does the entity provide security awareness and training to all new and existing members of its workforce? Obtain and review policies and procedures for security awareness and training program. Elements to review may include but are not limited to: • How workforce members are provided the security awareness and training • Identifies workforce members (including managers, senior executives, and as appropriate, business associates, and contractors) who will be provided with the security and awareness training • How workforce members will be provided with security and awareness training when there is a change in the entity's information systems • How frequently security awareness and training will be provided to all workforce members Obtain and review documentation demonstrating the implementation of a security awareness and training program including related training materials. Evaluate and determine whether the training program is reasonable and appropriate for workforce members to carry out their functions. Obtain and review documentation demonstrating that the security awareness and training programs are provided to the entire organization and made avail- able to independent contractors and business associates, if appropriate.	MPS Reviews policies and procedures surrounding training and awareness programs implemented throughout the organization.	Partial	MPS

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.312(a)(1)	§164.312(a)(1): Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	Access Control	Has the entity implemented technical policies and procedure for the electronic information systems that maintain ePHI to allow access only to authorized users? Does the entity only allow access to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4) to electronic information systems that maintain electronic protected health information? Obtain and review policies and procedures related to access control. Evaluate the content relative to the specified performance criteria to determine if ePHI is only accessible to authorized persons or software programs. Elements to review may include but are not limited to: • Identification of the capabilities of electronic information system access controls (i.e., read-only, modify, full access) • Identification of the type of access controls implemented for the electronic information systems • Identification of how system and generic IDs/ accounts are implemented, managed and controlled by technical access controls • Workforce members' roles and responsibilities regarding the capabilities to add, modify, or delete user access • The frequency of review and verification of user access to electronic information systems that maintain ePHI • The frequency of review and verification of software program access to electronic information systems that maintain ePHI • How is removed upon termination or modified upon change of position Obtain and review documentation demonstrating the implementation of access controls for electronic information systems that maintain ePHI. Evaluate and determine if the electronic information systems have the capacity to enable access controls; if access controls can be enabled, are the enabled access controls configured in accordance with the access control policies and procedures; and how are the electronic information systems' technical access capabilities defined (i.e., read-only, modify, full-access).	MPS reviews policies and procedures surrounding access controls to information systems.	Partial	MPS

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.312(a)(1) continued	§164.312(a)(1): Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	Access Control	Obtain and review documentation demonstrating a list of new workforce members from the electronic information system who was granted access to ePHI. Obtain and review documentation demonstrating the access levels granted to new workforce members. Evaluate and deter- mine whether workforce members' access was approved; review the new workforce members' technical access granted and compare it to approved user access to determine that technical access is approved and granted in accordance with the access authorization requirements. Obtain and review documentation of a list of users with privileged access. Evaluate and determine whether the privileged access is appropriate based on the access control policies. Obtain and review a list of default, generic/shared, and service accounts from the electronic information systems with access to ePHI. Obtain and review documentation demonstrating the access levels granted to default, generic/shared, and service accounts. Evaluate and determine if the default, generic/shared, and service accounts are in use and that access has been approved and granted in accordance with the access authorization requirements. Obtain and review documentation demonstrating that periodic reviews of procedures related to access controls have been conducted. Evaluate and determine whether reviews have been performed of user access levels and evaluate the content in relation to the specified performance criteria. Obtain and review documentation demonstrating a list of terminations and job transfers. Obtain documentation demonstrating the removal or modification of user access levels. Evaluate and determine whether user access level removal or modification was approved and performed in accordance with the related policies and procedures.	MPS reviews policies and procedures surrounding access controls to information systems.	Partial	MPS

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.312(a)(2)(i)	§164.312(a)(2)(i): Assign a unique name and/or number for identifying and tracking user identity.	Access Control – Unique User Identification	Does the entity have polices and procedures regarding the assignment of unique user IDs to track user identity? Does the entity assign unique user IDs to track user identity? Obtain and review policies and procedures regarding the assignment of unique user IDs. Evaluate the content of the policies and procedures in relation to the specified performance criteria to determine how user IDs are to be established and assigned. Obtain and review documentation demonstrating the assignment, creation, and use of unique user IDs in electronic information systems for user. Evaluate and determine if users are assigned a unique ID in accordance with the entity's policies and procedures for attributing new user IDs.	MPS reviews policies and procedures surrounding access controls to information systems.	Partial	MPS

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.312(a)(2)(iv)	§164.312(a)(2)(iv): Implement a mechanism to encrypt and decrypt electronic protected health information.	Access Control – Encryption and Decryption	Does the entity have policies and procedures in place to encrypt and decrypt ePHI including processes regarding the use and management of the confidential process or key used to encrypt and decrypt ePHI? Does the entity encrypt and decrypt ePHI including processes regarding the use and management of the confidential process or key used to encrypt and decrypt ePHI? Obtain and review the policies and procedures regarding the encryption and decryption of ePHI. Evaluate the content relative to the specified criteria to determine that the implementation and use of encryption appropriately protects ePHI. Elements to review may include but are not limited to: • Type(s) and documentation of encryption technology used for devices and media that contain or have access to ePHI • How the confidential processes or keys used for encryption and decryption are managed and protected • How access to modify or create keys is restricted to appropriate personnel Obtain and review documentation demonstrating ePHI being encrypted and decrypted. Evaluate and determine if ePHI is encrypted and decrypted in accordance with related policies and procedures. Has the entity chosen to implement an alternative measure? If yes, obtain and review entity documentation of why it has determined that the implementation specification is not a reasonable and appropriate safeguard and what equivalent alternative measure has been implemented instead. Evaluate documentation and assess whether the alternative measure implemented is equivalent to the protections afforded by the implementation specification.	MPS Reviews policies and procedures surrounding the encryption and decryption of ePHI.	Partial (we cannot verify encryption was in place) MPS reviews policies on organization's encryption/ decryption processes. Imprivata FairWarning's application can track if encryption was in place on risk of compromise form.	MPS/IM/ GR

Privacy audit protocol mapping	Established performance criteria	Key activity	Audit procedures	Imprivata FairWarning Patient Privacy Intelligence	Full or Partial	Imprivata FairWarning mapping
§164.316(b)(2) (iii)	§164.316(b)(2)(iii): Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information	Documentation – Updates	Does the entity have policies and procedures in place to perform periodic reviews and updates to Security Rule policies and procedures? Obtain and review policies and procedures regarding documentation reviews and updates. Obtain and review documents demonstrating that policies and procedures are reviewed and updated on a periodic basis. Evaluate and determine if such implementation is in accordance with related policies and procedures.	During the policy review, MPS looks at the policy on policies and how often policies have to be reviewed/ updated. We verify there is a process in place and the reviews and updates are documented. Additionally, MPS follows the industry and federal regulations and notifies customers when information changes	Partial	MPS