MAPPING GUIDE

NIST cybersecurity framework and ISO/IEC 27001 standard

imprivata®

NIST National Institute of Standards and Technolog Center of Excellence

What is NIST and the cybersecurity framework (CSF)?

The National Institute of Standards and Technology, a unit of the U.S. Commerce Department, promotes innovation and competitiveness by advancing standards, best practices, and guidelines in areas ranging from cybersecurity to laboratories to materials management.

In February 2013, the U.S. President issued Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” which directed NIST to work with stakeholders to develop a voluntary cybersecurity framework. This was done because of the recognition that federal agencies and critical infrastructures were facing growing security attacks and needed ways to help them better understand, organize, manage and mitigate security risks. The framework also provided a common language for agencies and infrastructure entities to communicate about security and risk management.

What is the purpose of the NIST CSF?

NIST defines the purpose of the CSF this way - “Helping organizations to better understand and improve their management of cybersecurity risk”. The Cybersecurity Framework is designed to assist practitioners to reduce cyber risks to critical infrastructure – defined as “Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these matters.”

While it was originally designed specifically for use by the U.S. federal agencies and critical infrastructure systems, many entities in both private and public sectors have adopted the framework as a helpful tool for organizing their security actions and mitigating cybersecurity risks.

How can my organization best use the NIST CSF and benefit from its use?

The Framework represents voluntary guidance founded on security best practices. Different sectors and individual organizations should customize the framework to best suit their risks, situations, and needs. The Framework should not be implemented as a checklist or a one-size-fits-all approach. To establish or improve upon its cybersecurity program, an organization should take a deliberate and customized approach to the CSF. The CSF provides for this seven step process to occur in an ongoing continuous improvement cycle:

1. Prioritize and scope
2. Orient
3. Create a current profile
4. Conduct a risk assessment
5. Create a target profile
6. Determine, analyze, and prioritize gaps
7. Implement action plan

With this deliberate process, an organization’s use of the NIST CSF can be a strong attestation to its diligence in managing and reducing risk.

How does Imprivata FairWarning assist with adherence to the NIST CSF?

Use of the Imprivata FairWarning solution assists customers in either fully or partially fulfilling over 75 Control Objectives across 22 categories and all of the five NIST functions. With this assistance, a customer's ability to demonstrate due care in protecting its sensitive data is strengthened.

NIST Function	NIST Category	Control Objective	Informative References	Imprivata FairWarning Solutions (Patient Privacy Intelligence and Cloud Security)	Imprivata FairWarning MPS	Imprivata FairWarning Provides Full or Partial Support
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	• CCS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8			
		ID.AM-2: Software platforms and applications within the organization are inventoried	• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8			
		ID.AM-3: Organizational communication and data flows are mapped	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8			
		ID.AM-4: External information systems are catalogued	• COBIT 5 APO02.02 • ISO/IEC 27001:2013 A.11.2.6 • NIST SP 800-53 Rev. 4 AC-20, SA-9			
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• COBIT 5 APO03.03, APO03.04, BAI09.02 • ISA 62443-2-1:2009 4.2.3.6 • ISO/IEC 27001:2013 A.8.2.1 • NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14	Imprivata FairWarning helps customers classify and prioritize their information assets that contain ePHI. This assistance occurs during onboarding and with data sources that are added by existing customers.		Partial
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• COBIT 5 APO01.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1 • NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11			

NIST Function	NIST Category	Control Objective	Informative References	Imprivata FairWarning Solutions (Patient Privacy Intelligence and Cloud Security)	Imprivata FairWarning MPS	Imprivata FairWarning Provides Full or Partial Support
IDENTIFY (ID)	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-1: The organization's role in the supply chain is identified and communicated	• COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 • ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 • NIST SP 800-53 Rev. 4 CP-2, SA-12	Imprivata FairWarning helps monitor non-employee service providers' access to and activities around customer ePHI and other confidential data.	The MPS team monitors non-employee service providers' access to and activities around customer ePHI and other confidential data.	Partial
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	• COBIT 5 APO02.06, APO03.01 • NIST SP 800-53 Rev. 4 PM-8			
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	• COBIT 5 APO02.01, APO02.06, APO03.01 • ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 • NIST SP 800-53 Rev. 4 PM-11, SA-14			
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	• ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 • NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14			
		ID.BE-5: Resilience requirements to support delivery of critical services are established	• COBIT 5 DSS04.02 • ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 • NIST SP 800-53 Rev. 4 CP-2, CP- 11, SA-14			
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1: Organizational information security policy is established	• COBIT 5 APO01.03, EDM01.01, EDM01.02 • ISA 62443-2-1:2009 4.3.2.6 • ISO/IEC 27001:2013 A.5.1.1 • NIST SP 800-53 Rev. 4 -1 controls from all families			

NIST Function	NIST Category	Control Objective	Informative References	Imprivata FairWarning Solutions (Patient Privacy Intelligence and Cloud Security)	Imprivata FairWarning MPS	Imprivata FairWarning Provides Full or Partial Support
IDENTIFY (ID)	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	• COBIT 5 APO13.12 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 • NIST SP 800-53 Rev. 4 PM-1, PS-7			
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	• COBIT 5 MEA03.01, MEA03.04 • ISA 62443-2-1:2009 4.4.3.7 • ISO/IEC 27001:2013 A.18.1 • NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)	Imprivata FairWarning helps customers comply with HIPAA access rights management, PCI DSS, and other regulatory requirements.		Partial
		ID.GV-4: Governance and risk management processes address cybersecurity risks	• COBIT 5 DSS04.02 • ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 • NIST SP 800-53 Rev. 4 PM-9, PM-11			
	Risk Assessment (ID. RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1: Asset vulnerabilities are identified and documented	• CCS CSC 4 • COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 • ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 • ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CA- 8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5			
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	• ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 • ISO/IEC 27001:2013 A.6.1.4 • NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5			
		ID.RA-3: Threats, both internal and external, are identified and documented	• COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 • ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 • NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16	Imprivata FairWarning helps customers monitor and investigate possible internal and external threats to its ePHI and other confidential data.	MPS staff monitors and investigates possible internal and external threats to its ePHI and other confidential data.	Partial

NIST Function	NIST Category	Control Objective	Informative References	Imprivata FairWarning Solutions (Patient Privacy Intelligence and Cloud Security)	Imprivata FairWarning MPS	Imprivata FairWarning Provides Full or Partial Support
IDENTIFY (ID)	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-4: Potential business impacts and likelihoods are identified	• COBIT 5 DSS04.02 • ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 • NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14			
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	• COBIT 5 APO12.02 • ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16			
		ID.RA-6: Risk responses are identified and prioritized	• COBIT 5 APO12.05, APO13.02 • NIST SP 800-53 Rev. 4 PM-4, PM-9			
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	• COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 • ISA 62443-2-1:2009 4.3.4.2 • NIST SP 800-53 Rev. 4 PM-9			
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.3.2.6.5 • NIST SP 800-53 Rev. 4 PM-9			
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	• NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14			

NIST Function	NIST Category	Control Objective	Informative References	Imprivata FairWarning Solutions (Patient Privacy Intelligence and Cloud Security)	Imprivata FairWarning MPS	Imprivata FairWarning Provides Full or Partial Support
PROTECT (PR)	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-1: Identities and credentials are managed for authorized devices and users	• CCS CSC 16 • COBIT 5 DSS05.04, DSS06.03 • ISA 62443-2-1:2009 4.3.3.5.1 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 • NIST SP 800-53 Rev. 4 AC-2, IA Family	Imprivata FairWarning helps manage user credentials by monitoring user access and alerting customers to potential issues.	Imprivata FairWarning helps manage user credentials by monitoring user access and alerting customers to potential issues.	Partial
		PR.AC-2: Physical access to assets is managed and protected	• COBIT 5 DSS01.04, DSS05.05 • ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 • ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 • NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9	Imprivata FairWarning can help manage and protect physical access to assets, depending on data input from customer. For example, if customer sends data from its badge access systems, Imprivata FairWarning can assist with physical access issues.	Imprivata FairWarning can help manage and protect physical access to assets, depending on data input from customer. For example, if customer sends data from its badge access systems, Imprivata FairWarning can assist with physical access issues. MPS will monitor use of user credentials and escalate issues to customer as needed.	Partial
		PR.AC-3: Remote access is managed	• COBIT 5 APO13.01, DSS01.04, DSS05.03 • ISA 62443-2-1:2009 4.3.3.6.6 • ISA 62443-3-3:2013 SR 1.13, SR 2.6 • ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1 • NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20	Imprivata FairWarning can help manage remote access to assets, depending on data input from customer. For example, if customer sends data from its remote access management systems, FairWarning can assist with remote access issues.	Imprivata FairWarning can help manage remote access to assets, depending on data input from customer. For example, if customer sends data from its remote access management systems, FairWarning can assist with remote access issues. MPS will monitor use of user credentials and escalate issues to customer as needed.	Partial
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	• CCS CSC 12, 15 • ISA 62443-2-1:2009 4.3.3.7.3 • ISA 62443-3-3:2013 SR 2.1 • ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 • NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16	Imprivata FairWarning helps user access and activity to ensure access permissions are being maintained.	Imprivata FairWarning helps user access and activity to ensure access permissions are being maintained. MPS will monitor use of user credentials and escalate issues to customer as needed.	Partial

NIST Function	NIST Category	Control Objective	Informative References	Imprivata FairWarning Solutions (Patient Privacy Intelligence and Cloud Security)	Imprivata FairWarning MPS	Imprivata FairWarning Provides Full or Partial Support
PROTECT (PR)	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	• ISA 62443-2-1:2009 4.3.3.4 • ISA 62443-3-3:2013 SR 3.1, SR 3.8 • ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, SC-7			
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-1: All users are informed and trained	• CCS CSC 9 • COBIT 5 APO07.03, BAI05.07 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.7.2.2 • NIST SP 800-53 Rev. 4 AT-2, PM-13	Use of Imprivata FairWarning supports user education on acceptable compliance and security practices in two ways: 1) user knowledge that organization is regularly reviewing access will affect behavior, and 2) remediation actions against unacceptable actions will foster acceptable compliance and security.		Partial
		PR.AT-2: Privileged users understand roles & responsibilities	• CCS CSC 9 • COBIT 5 APO07.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 AT-3, PM-13	Regular review of access by privileged users (and remediation of unacceptable access) will help these users understand their roles and responsibilities.	MPS analysts regularly review privileged user access and remediate unacceptable access. This review will help these users understand their roles and responsibilities.	Partial
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	• CCS CSC 9 • COBIT 5 APO07.03, APO10.04, APO10.05 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 PS-7, SA-9	Imprivata FairWarning helps customers monitor the access and activities of third-party stakeholders to customer ePHI and other confidential data.	MPS staff would monitor the access and activities of third-party stakeholders to customer ePHI and other confidential data.	Partial
		PR.AT-4: Senior executives understand roles & responsibilities	• CCS CSC 9 • COBIT 5 APO07.03 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 AT-3, PM-13	Regular review of access by senior executive users (and remediation of unacceptable access) will help these users understand their roles and responsibilities.	MPS analysts perform regular reviews of senior executive user access and remediate unacceptable access. This review will help these users understand their roles and responsibilities.	Partial

NIST Function	NIST Category	Control Objective	Informative References	Imprivata FairWarning Solutions (Patient Privacy Intelligence and Cloud Security)	Imprivata FairWarning MPS	Imprivata FairWarning Provides Full or Partial Support
PROTECT (PR)	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-5: Physical and information security personnel understand roles & responsibilities	• CCS CSC 9 • COBIT 5 APO07.03 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 AT-3, PM-13	Regular review of access by physical and information security users (and remediation of unacceptable access) will help these users understand their roles and responsibilities.	MPS analysts perform regular reviews of physical and information security user access and remediate unacceptable access. This review will help these users understand their roles and responsibilities.	Partial
	Data Security (PR. DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-1: Data-at-rest is protected	• CCS CSC 17 • COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06 • ISA 62443-3-3:2013 SR 3.4, SR 4.1 • ISO/IEC 27001:2013 A.8.2.3 • NIST SP 800-53 Rev. 4 SC-28			
		PR.DS-2: Data-in- transit is protected	• CCS CSC 17 • COBIT 5 APO01.06, DSS06.06 • ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 • ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev. 4 SC-8			
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	• COBIT 5 BAI09.03 • ISA 62443-2-1:2009 4. 4.3.3.3.9, 4.3.4.4.1 • ISA 62443-3-3:2013 SR 4.2 • ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 • NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16			
		PR.DS-4: Adequate capacity to ensure availability is maintained	• COBIT 5 APO13.01 • ISA 62443-3-3:2013 SR 7.1, SR 7.2 • ISO/IEC 27001:2013 A.12.3.1 • NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5			

NIST Function	NIST Category	Control Objective	Informative References	Imprivata FairWarning Solutions (Patient Privacy Intelligence and Cloud Security)	Imprivata FairWarning MPS	Imprivata FairWarning Provides Full or Partial Support
PROTECT (PR)	Data Security (PR. DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-5: Protections against data leaks are implemented	• CCS CSC 17 • COBIT 5 APO01.06 • ISA 62443-3-3:2013 SR 5.2 • ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4	Imprivata FairWarning helps customers monitor and investigate inappropriate access to ePHI and other confidential data. With this assistance, customers can be protected from data exfiltration attempts such as identity theft or medical identity theft of confidential data.	The MPS staff monitors and investigates inappropriate access to customer ePHI and other confidential data. With this assistance, customers can be protected from data exfiltration attempts such as identity theft or medical identity theft of confidential data.	Partial
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	• ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 • ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev. 4 SI-7			
		PR.DS-7: The development and testing environment(s) are separate from the production environment	• COBIT 5 BAI07.04 • ISO/IEC 27001:2013 A.12.1.4 • NIST SP 800-53 Rev. 4 CM-2			
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-1: A baseline configuration of information technology/ industrial control systems is created and maintained	• CCS CSC 3, 10 • COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 • ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 • ISA 62443-3-3:2013 SR 7.6 • ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10			

NIST Function	NIST Category	Control Objective	Informative References	Imprivata FairWarning Solutions (Patient Privacy Intelligence and Cloud Security)	Imprivata FairWarning MPS	Imprivata FairWarning Provides Full or Partial Support
PROTECT (PR)	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-2: A System Development Life Cycle to manage systems is implemented	• COBIT 5 APO13.01 • ISA 62443-2-1:2009 4.3.4.3.3 • ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 • NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8			
		PR.IP-3: Configuration change control processes are in place	• COBIT 5 BAI06.01, BAI01.06 • ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 • ISA 62443-3-3:2013 SR 7.6 • ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10			
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	• COBIT 5 APO13.01 • ISA 62443-2-1:2009 4.3.4.3.9 • ISA 62443-3-3:2013 SR 7.3, SR 7.4 • ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 • NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9			
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	• COBIT 5 DSS01.04, DSS05.05 • ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 • ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 • NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18			
		PR.IP-6: Data is destroyed according to policy	• COBIT 5 BAI09.03 • ISA 62443-2-1:2009 4.3.4.4.4 • ISA 62443-3-3:2013 SR 4.2 • ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 • NIST SP 800-53 Rev. 4 MP-6			
		PR.IP-7: Protection processes are continuously improved	• COBIT 5 APO11.06, DSS04.05 • ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6			

NIST Function	NIST Category	Control Objective	Informative References	Imprivata FairWarning Solutions (Patient Privacy Intelligence and Cloud Security)	Imprivata FairWarning MPS	Imprivata FairWarning Provides Full or Partial Support
PROTECT (PR)	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	• ISO/IEC 27001:2013 A.16.1.6 • NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4			
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	• COBIT 5 DSS04.03 • ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 • ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2 • NIST SP 800-53 Rev. 4 CP-2, IR-8			
		PR.IP-10: Response and recovery plans are tested	• ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 • ISA 62443-3-3:2013 SR 3.3 • ISO/IEC 27001:2013 A.17.1.3 • NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14			
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	• COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 • ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 • ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4 • NIST SP 800-53 Rev. 4 PS Family	Imprivata FairWarning helps customers monitor and provides alerts on any actions of terminated employees; this helps customers quickly correct any deprovisioning errors. In addition, Imprivata FairWarning can provide alerts on departing employees that provide supplemental reporting on specific activities such as downloads, hard deletes, print activity, and large reports run. Imprivata FairWarning can also be integrated with SailPoint for full lifecycle identity and access management (IAM).	Imprivata FairWarning helps customers monitor and provides alerts on any actions of terminated employees; this helps customers quickly correct any deprovisioning errors. In addition, Imprivata FairWarning can provide alerts on departing employees that provide supplemental reporting on specific activities such as downloads, hard deletes, print activity, and large reports run. Imprivata FairWarning can also be integrated with SailPoint for full lifecycle IAM.	Partial

NIST Function	NIST Category	Control Objective	Informative References	Imprivata FairWarning Solutions (Patient Privacy Intelligence and Cloud Security)	Imprivata FairWarning MPS	Imprivata FairWarning Provides Full or Partial Support
PROTECT (PR)	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-12: A vulnerability management plan is developed and implemented	• ISO/IEC 27001:2013 A.12.6.1, A.18.2.2 • NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2	Imprivata FairWarning helps its customers provide vulnerability management for audit control and access rights issues.		Partial
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	• COBIT 5 BAI09.03 • ISA 62443-2-1:2009 4.3.3.3.7 • ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5 • NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5			
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	• COBIT 5 DSS05.04 • ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 • ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 • NIST SP 800-53 Rev. 4 MA-4	Imprivata FairWarning helps monitor remote access to assets, depending on data input from customer. For example, if customer sends data from its remote management access systems, FairWarning will assist with remote access management.	Imprivata FairWarning's MPS staff monitors remote access to assets, depending on data input from customer. For example, if customer sends data from its remote management access systems, MPS staff will perform remote access management.	Partial

NIST Function	NIST Category	Control Objective	Informative References	Imprivata FairWarning Solutions (Patient Privacy Intelligence and Cloud Security)	Imprivata FairWarning MPS	Imprivata FairWarning Provides Full or Partial Support
PROTECT (PR)	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-1: Audit/ log records are determined, documented, implemented, and reviewed in accordance with policy	• CCS CSC 14 • COBIT 5 APO11.04 • ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 • ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 • ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 • NIST SP 800-53 Rev. 4 AU Family	Imprivata FairWarning works with customers to extract, document, and review audit logs from ePHI containing data sources and authoritative user sources. This compiled log information is then used to determine if user access conforms to customer compliance and security policies.	Imprivata FairWarning works with customers to extract, document, and review audit logs from ePHI containing data sources and authoritative user sources. This compiled log information is then used to determine if user access conforms to customer compliance and security policies. MPS provides this initial access analysis and then escalates to customer as needed.	Full
		PR.PT-2: Removable media is protected and its use restricted according to policy	• COBIT 5 DSS05.02, APO13.01 • ISA 62443-3-3:2013 SR 2.3 • ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 • NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7			
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	• COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 • ISO/IEC 27001:2013 A.9.1.2 • NIST SP 800-53 Rev. 4 AC-3, CM-7	Imprivata FairWarning helps customers monitor their users' access and activity based on event monitoring within their audit logs. Customers can monitor this access and activity by running reports within the app itself. In addition, FairWarning customers can better identify whether users have higher privileges or level of data access than required for role/job function.	Imprivata FairWarning helps customers monitor their users' access and activity based on event monitoring within their audit logs. MPS monitors this access and activity by running reports within the app itself and escalating issues to customer as needed.	Full
		PR.PT-4: Communications and control networks are protected	• CCS CSC 7 • COBIT 5 DSS05.02, APO13.01 • ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 • ISO/IEC 27001:2013 A.13.1.1, A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, AC-17, AC- 18, CP-8, SC-7			

NIST Function	NIST Category	Control Objective	Informative References	Imprivata FairWarning Solutions (Patient Privacy Intelligence and Cloud Security)	Imprivata FairWarning MPS	Imprivata FairWarning Provides Full or Partial Support
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	• COBIT 5 DSS03.01 • ISA 62443-2-1:2009 4.4.3.3 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4			
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	• ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 • ISO/IEC 27001:2013 A.16.1.1, A.16.1.4 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4	Imprivata FairWarning helps customers monitor and analyze events that may suggest an imminent attack. Customers can monitor this access and activity by running reports within the app.	Imprivata FairWarning's MPS staff monitors and analyzes events that may suggest attack.	Full
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	• ISA 62443-3-3:2013 SR 6.1 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4	Imprivata FairWarning Dynamic Identity Intelligence links multiple authoritative user data sources and clinical application event logs to build a comprehensive profile of customer users and activities.		Full
		DE.AE-4: Impact of events is determined	• COBIT 5 APO12.06 • NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI -4	Imprivata FairWarning helps customers investigate inappropriate data access and determine its scope and impact.	Imprivata FairWarning's MPS staff investigates inappropriate data access and helps customers determine its scope and impact.	Partial
		DE.AE-5: Incident alert thresholds are established	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.2.3.10 • NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8	Imprivata FairWarning helps customers evaluate the correct thresholds for incidents (particularly trending thresholds).	Imprivata FairWarning's MPS staff establishes thresholds for incidents (particularly trending thresholds) after consultation with and direction from the customer.	Partial

NIST Function	NIST Category	Control Objective	Informative References	Imprivata FairWarning Solutions (Patient Privacy Intelligence and Cloud Security)	Imprivata FairWarning MPS	Imprivata FairWarning Provides Full or Partial Support
DETECT (DE)	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cybersecurity events	• CCS CSC 14, 16 • COBIT 5 DSS05.07 • ISA 62443-3-3:2013 SR 6.2 • NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4	Imprivata FairWarning helps customers monitor for events at the application security level. In addition, it can interface data into other security monitoring tools (e.g., SIEM).	Imprivata FairWarning's MPS staff monitors for events occurring at the application security level. In addition, it can interface data into other security monitoring tools (e.g., SIEM).	Partial
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	• ISA 62443-2-1:2009 4.3.3.3.8 • NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20			
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	• ISA 62443-3-3:2013 SR 6.2 • ISO/IEC 27001:2013 A.12.4.1 • NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	Imprivata FairWarning helps customers monitor their personnel's data access activity.	Imprivata FairWarning MPS monitors the customer personnel's data access and activity and escalates issues to customers as needed.	Full
		DE.CM-4: Malicious code is detected	• CCS CSC 5 • COBIT 5 DSS05.01 • ISA 62443-2-1:2009 4.3.4.3.8 • ISA 62443-3-3:2013 SR 3.2 • ISO/IEC 27001:2013 A.12.2.1 • NIST SP 800-53 Rev. 4 SI-3			
		DE.CM-5: Unauthorized mobile code is detected	• ISA 62443-3-3:2013 SR 2.4 • ISO/IEC 27001:2013 A.12.5.1 • NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44			
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	• COBIT 5 APO07.06 • ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 • NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4	Imprivata FairWarning helps customers monitor the data access activity of external service providers. This monitoring helps customers detect potential cybersecurity events.	Imprivata FairWarning monitors the data access and activity of customers' external service providers, escalating to the customer as needed. This helps customers detect potential cybersecurity events.	Partial

NIST Function	NIST Category	Control Objective	Informative References	Imprivata FairWarning Solutions (Patient Privacy Intelligence and Cloud Security)	Imprivata FairWarning MPS	Imprivata FairWarning Provides Full or Partial Support
DETECT (DE)	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	• NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	Imprivata FairWarning helps customers monitor for unauthorized users accessing their confidential data.	Imprivata FairWarning MPS monitors for unauthorized user access of confidential data, escalating potential cybersecurity events to the customer as needed.	Partial
		DE.CM-8: Vulnerability scans are performed	• COBIT 5 BAI03.10 • ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 • ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev. 4 RA-5			
	Detection Processes (DE. DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	• CCS CSC 5 • COBIT 5 DSS05.01 • ISA 62443-2-1:2009 4.4.3.1 • ISO/IEC 27001:2013 A.6.1.1 • NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14			
		DE.DP-2: Detection activities comply with all applicable requirements	• ISA 62443-2-1:2009 4.4.3.2 • ISO/IEC 27001:2013 A.18.1.4 • NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4	Imprivata FairWarning monitors user access and detects potential issues helping customers comply with requirements related to data, privacy protection, acceptable use, and security.		Partial
		DE.DP-3: Detection processes are tested	• COBIT 5 APO13.02 • ISA 62443-2-1:2009 4.4.3.2 • ISA 62443-3-3:2013 SR 3.3 • ISO/IEC 27001:2013 A.14.2.8 • NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4			
		DE.DP-4: Event detection information is communicated to appropriate parties	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.3.4.5.9 • ISA 62443-3-3:2013 SR 6.1 • ISO/IEC 27001:2013 A.16.1.2 • NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4			
		DE.DP-5: Detection processes are continuously improved	• COBIT 5 APO11.06, DSS04.05 • ISA 62443-2-1:2009 4.4.3.4 • ISO/IEC 27001:2013 A.16.1.6 • NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14			

NIST Function	NIST Category	Control Objective	Informative References	Imprivata FairWarning Solutions (Patient Privacy Intelligence and Cloud Security)	Imprivata FairWarning MPS	Imprivata FairWarning Provides Full or Partial Support
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	RS.RP-1: Response plan is executed during or after an event	•COBIT 5 BAI01.10 •CCS CSC 18 •ISA 62443-2-1:2009 4.3.4.5.1 •ISO/IEC 27001:2013 A.16.1.5 •NIST SP 800-53 Rev. 4 CP-2, CP-10,IR-4, IR-8			
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies	RS.CO-1: Personnel know their roles and order of operations when a response is needed	•ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 •ISO/IEC 27001:2013 A.6.1.1, A.16.1.1 •NIST SP 800-53 Rev. 4 CP-2, CP-3,IR-3, IR-8			
		RS.CO-2: Events are reported consistent with established criteria	•ISA 62443-2-1:2009 4.3.4.5.5 •ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 •NIST SP 800-53 Rev. 4 AU-6, IR-6,IR-8	Imprivata FairWarning provides enforced policies (within its solution) that can monitor for certain events (e.g, neighbor snooping, patient of interest, etc.) These enforced policies can be edited to alert customers when they detect certain suspicious activity.	Imprivata FairWarning's MPS staff builds and monitors enforced policies (within the FairWarning solution) that can detect certain events (e.g, neighbor snooping, patient of interest, etc.) These enforced policies trigger alerts when certain suspicious activity is detected, and MPS staff investigates those alerts.	Partial
		RS.CO-3: Information is shared consistent with response plans	• ISA 62443-2-1:2009 4.3.4.5.2 • ISO/IEC 27001:2013 A.16.1.2 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4			
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	• ISA 62443-2-1:2009 4.3.4.5.5 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8			

NIST Function	NIST Category	Control Objective	Informative References	Imprivata FairWarning Solutions (Patient Privacy Intelligence and Cloud Security)	Imprivata FairWarning MPS	Imprivata FairWarning Provides Full or Partial Support
RESPOND (RS)	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	• NIST SP 800-53 Rev. 4 PM-15, SI-5			
	Analysis (RS. AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-1: Notifications from detection systems are investigated	• COBIT 5 DSS02.07 • ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • ISA 62443-3-3:2013 SR 6.1 • ISO/IEC 27001:2013 A.12.4.1,A.12.4.3, A.16.1.5 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4	Imprivata FairWarning detects inappropriate data access and provides alerts, which prompt the customer to investigate possible incidents.	Imprivata FairWarning's MPS staff monitors alerts on inappropriate data access.	Partial
		RS.AN-2: The impact of the incident is understood	• ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • ISO/IEC 27001:2013 A.16.1.6 • NIST SP 800-53 Rev. 4 CP-2, IR-4	Through its investigation module, Imprivata FairWarning helps customers understand the impact of data security incidents.	Through the Imprivata FairWarning investigation module, the MPS staff construct reports to understand and illustrate the impact of data security incidents.	Partial
		RS.AN-3: Forensics are performed	• ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 • ISO/IEC 27001:2013 A.16.1.7 • NIST SP 800-53 Rev. 4 AU-7, IR-4	Through its investigation module, Imprivata FairWarning helps customers investigate and determine root causes for data access incidents.	Through the Imprivata FairWarning investigation module, the MPS staff investigates and determines root causes for data access incidents	Partial
		RS.AN-4: Incidents are categorized consistent with response plans	• ISA 62443-2-1:2009 4.3.4.5.6 • ISO/IEC 27001:2013 A.16.1.4 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8	Through its investigation module, Imprivata FairWarning helps customers understand the impact of data access incidents.	Through the Imprivata FairWarning investigation module, the MPS staff construct reports to understand and illustrate data access incidents and categorize them.	Partial

NIST Function	NIST Category	Control Objective	Informative References	Imprivata FairWarning Solutions (Patient Privacy Intelligence and Cloud Security)	Imprivata FairWarning MPS	Imprivata FairWarning Provides Full or Partial Support
RESPOND (RS)	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	RS.MI-1: Incidents are contained	• ISA 62443-2-1:2009 4.3.4.5.6 • ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 IR-4	Through its investigation module, Imprivata FairWarning helps customers understand the impact of data access. Customers can better contain incidents with this knowledge.		Partial
		RS.MI-2: Incidents are mitigated	• ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 • ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 • NIST SP 800-53 Rev. 4 IR-4	Through its investigation module, Imprivata FairWarning helps customers understand the impact of data access. Customers can better mitigate incidents with this knowledge.		
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	• ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5			
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/ response activities.	RS.IM-1: Response plans incorporate lessons learned	• COBIT 5 BAI01.13 • ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 • ISO/IEC 27001:2013 A.16.1.6 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8			
		RS.IM-2: Response strategies are updated	• NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8			
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	RC.RP-1: Recovery plan is executed during or after an event	• CCS CSC 8 • COBIT 5 DSS02.05, DSS03.04 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8			

NIST Function	NIST Category	Control Objective	Informative References	Imprivata FairWarning Solutions (Patient Privacy Intelligence and Cloud Security)	Imprivata FairWarning MPS	Imprivata FairWarning Provides Full or Partial Support
RECOVER (RC)	Improvements (RC. IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned	• COBIT 5 BAI05.07 • ISA 62443-2-1 4.4.3.4 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8			
		RC.IM-2: Recovery strategies are updated	• COBIT 5 BAI07.08 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8			
	Communications (RC. CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	RC.CO-1: Public relations are managed	• COBIT 5 EDM03.02			
		RC.CO-2: Reputation after an event is repaired	• COBIT 5 MEA03.02			
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	• NIST SP 800-53 Rev. 4 CP-2, IR-4			

MAPPING GUIDE

Mapping to ISO/IEC 27001

Background on the ISO/IEC 27001:2013 standard

ISO/IEC 27001:2013 is an international standard that describes best practices for an information security management system (ISMS). As defined by the ISO organization, the ISO standards "will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties." https://www.iso.org/isoiec-27001-information-security.html

It is commonly known as ISO 27001 (ISO = Intranational Organization for Standardization).
The ISO organization is based in Geneva, Switzerland. The most recent version of the ISO 27001 standard was published in September 2013.

Purpose of an information security management system

An information security management system (ISMS) is a set of frameworks that contain policies and procedures for tackling security risks in an organization. The focus of an ISMS is to ensure business continuity by minimizing all security risks to information assets and limiting security breach impacts to a bare minimum.

The ISO 27001 standard describes how an ISMS can be built at an organization. Through implementation, it requires the organization to develop a set of information security rules, responsibilities, and controls, which then enable the organization to manage its complex systems and the security risk that arises from them.

Other ISO standards

In addition to ISO 27001, there is the ISO 27002 standard. Whereas the ISO 27001 standards states and defines the audit requirements, ISO 27002 provides best practice recommendations on the implementation of information security management by those who are responsible for implementing or maintaining the ISMS. As the ISO Organization states, the ISO 27002 is a "code of practice - a generic, advisory document, not a formal specification such as ISO/IEC 27001". ISO 27002 recommends information security controls addressing information security control objectives arising from risks to the confidentiality, integrity, and availability of information.
The items in ISO 27002 are the same as items in ISO 27001's Annex A. Each control from Annex A exists in ISO 27002, together with a more detailed explanation of how to implement it.

Addressing ISO 27001 through use of Imprivata FairWarning

For clarity in showing how Imprivata FairWarning's capabilities assist in ISO 27001 implementation and support, the items in Annex A are presented below.

The annex is not required of organizations implementing ISO 27001. This means that certified organizations are expected to use it, but they are free to deviate from or supplement it to address their specific information risks.

ISO 27001's Annex A contains the groups, objectives, and controls associated with the standard. Specifically, there are now 114 controls in 14 groups and 35 control objectives within the 2013 version.

Note that this document contains only a subsection of the Annex A items that are supported (in full or partially) by Impriavata FairWarning's Patient Privacy Intelligence (PPI) and Managed Privacy Services (MPS) capabilities.

*A.5: Information security policies
*A.6: Organization of information security
*A.7: Human resource security
*A.8: Asset management
*A.9: Access control A.10: Cryptography
A.11: Physical and environmental security
*A.12: Operations security A.13: Communications security
*A.14: System acquisition, development and maintenance
*A.15: Supplier relationships
*A.16: Information security incident management
A.17: Information security aspects of business continuity management
*A.18: Compliance (with internal requirements, such as policies, and with external requirements, such as laws)

In this report of Imprivata FairWarning's applicability and full or partial support of ISO 27001, we focus on 40 controls that are within the groups starred above.

Section	Requirement	Control	Imprivata FairWarning Platform	Imprivata FairWarning Provides Full or Partial Support
A.5 Information security policies A.5.1 Management direction for information security Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.				
A.5.1.2	Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	As part of the onboarding process with Imprivata FairWarning, customers determine and deploy alerts that monitor access rights management. These FairWarning alerts assist the customer in the development and encirclement of their organization's privacy and security policies.	Full
A.6 Organization of information security A.6.1 Internal organization Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.				
A.6.1.1	Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.	Customer uses workflows for incident response management within the FairWarning application. These incidents assist the customer in defining incidents and assigning applicable staff to remediate.	Full

Section	Requirement	Control	Imprivata FairWarning Platform	Imprivata FairWarning Provides Full or Partial Support
A.7 Human resource security A.7.2 During employment Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.				
A.7.2.1	Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	Imprivata FairWarning assists customers in two ways with this control. First, the customer can gain insight into data access and usage of its account holders. This helps them ensure their privacy and security policies and procedures are being met. Secondly, Imprivata FairWarning provides educational material to customers. These materials assist managers in setting expectations with their staff about what will be monitored via FairWarning. This education and monitoring assist in moving customer culture towards optimal compliance and security practices.	Full
A.7.2.3	Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	Imprivata FairWarning provides incident response tracking and management through forensically sound data. If incident is determined by customer to be due to an employee security breach, information provided by FairWarning may be used in a disciplinary process.	Full
A.8 Asset management A.8.1 Responsibility for assets Objective: To identify organizational assets and define appropriate protection responsibilities.				
A.8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	Customers use the Imprivata FairWarning application to monitor access to confidential information such as PHI, PII, and/or intellectual property. This monitoring assists customers in both 1) identifying and documenting violations of appropriate access to confidential data and 2) implementing security controls to enforce appropriate access. This monitoring and any associated remediation of inappropriate access helps ensure acceptable use of the confidential information.	Full
A.8.2 Information classification Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.				
A.8.2.1	Classification of information	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.	As part of its onboarding process with Imprivata FairWarning, the customer prioritizes information in highest need of user access monitoring. The customer may prioritize information because the criticality of the applications, legal requirements or other values.	Full

Section	Requirement	Control	Imprivata FairWarning Platform	Imprivata FairWarning Provides Full or Partial Support
A.9 Access control A.9.1 Business requirements of access control Objective: To limit access to information and information processing facilities.				
A.9.1.1	Access control policy	An access control policy shall be established, documented and reviewed based on business and information security requirements.	Imprivata FairWarning assists customers, through the use of behavioral analytics, in the detection of access violations as specified by the customer's policies. This provides customers insight into what their users are accessing. With this information, customers may craft access control policies that meet their business and security requirements.	Full
A.9.1.2	Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	Customer may use Imprivata FairWarning's platform to gain visibility into the data access patterns of their users. Based on that information, customers can remediate access violations and ensure authorized access and use.	Full
A.9.2 User access management Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.				
A.9.2.5	Review of user access rights	Asset owners shall review users' access rights at regular intervals.	Imprivata FairWarning assists its customers in regularly monitoring what information their users are accessing. The Imprivata FairWarning platform can aid in determining who is currently accessing what (documenting) and provide evidence to support establishing and changing access control policies.	Full
A.9.2.6	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Customers may use Imprivata FairWarning to monitor if terminated employees are accessing data. This alerting can help customers identify any gaps in their employee deprovisioning process that allow for continued access after termination.	Full
A.9.4 System and application access control Objective: To prevent unauthorized access to systems and applications.				
A.9.4.1	Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	Imprivata FairWarning assists its customers to regularly monitor what information their users are accessing. The Imprivata FairWarning platform can aid in determining who is currently accessing what, documenting and providing evidence to support establishing and changing of access control policies.	Partial

Section	Requirement	Control	Imprivata FairWarning Platform	Imprivata FairWarning Provides Full or Partial Support
A.9.4.2	Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	Imprivata FairWarning can provide customers information on how, when, from where, etc. users are logging into systems. This data assists customers in identifying if secure logon procedures are met.	Partial
A.12 Operations security A.12.2 Protection from malware Objective: To ensure that information and information processing facilities are protected against malware.				
A.12.2.1	Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Imprivata FairWarning application helps customers detect potential security violations and provides incident tracking and management. This allows for full documentation of post-incident analysis, resolution, mitigation, and other activities. Imprivata FairWarning can detect file manipulation, compromised account credentials, and other changes which may be indicative of malware infection.	Partial
A.12.3 Backup Objective: To protect against loss of data.				
A.12.3.1	Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	For its SaaS customers, Imprivata FairWarning maintains backup copies of audit files for monitored data sources. Restoration of these backup files is tested regularly.	Partial
A.12.4 Logging and monitoring Objective: To record events and generate evidence.				
A.12.4.1	Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	Through their use of the Imprivata FairWarning platform, a customer may keep and regularly review the event logs of monitored data sources.	Full
A.12.4.2	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	Through ongoing health check monitoring, Imprivata FairWarning ensures the integrity and confidentiality of audit logs it receives from customers.	Partial
A.12.4.3	Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	A customer may use the Imprivata FairWarning platform to log and regularly review the access patterns of its administrators and operators.	Full
A.12.4.4	Clock synchronisation	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.	Imprivata FairWarning synchronizes data logs it receives from customers to a single reference time source.	Full

Section	Requirement	Control	Imprivata FairWarning Platform	Imprivata FairWarning Provides Full or Partial Support
A.12.5 Control of operational software Objective: To ensure the integrity of operational systems.				
A.12.5.1	Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.	Imprivata FairWarning provides information to customers on the installation of software on select monitored data sources. Customers may use this information to implement controls to block these installations.	Partial
A.12.7 Information systems audit considerations Objective: To minimise the impact of audit activities on operational systems.				
A.12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	Imprivata FairWarning's platform and audit extraction processes are planned and implemented to minimize any disruptions to customers and their business processes.	Full
A.14 System acquisition, development and maintenance A.14.1 Security requirements of information systems Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.				
A.14.1.2	Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	When obtaining data from customers over public networks, Imprivata FairWarning employs secure protocols and dedicated communication channels. These practices protect transmitted information integrity and confidentiality.	Full
A.14.1.3	Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	When obtaining data from customers over public networks, Imprivata FairWarning employs secure protocols and dedicated communication channels. These practices protect transmitted information integrity and confidentiality.	Full
A.14.2 Security in development and support processes Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.				
A.14.2.2	System change control procedures	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	Any updates to the Imprivata FairWarning application go through a formal change control process internally. Customers are kept updated on these changes and may elect to use their own change control procedures for changes to their production of FairWarning applications.	Full

Section	Requirement	Control	Imprivata FairWarning Platform	Imprivata FairWarning Provides Full or Partial Support
A.14.2.3	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	All updates to the Imprivata FairWarning application go through an extensive quality assurance process before being made available to customers.	Full
A.14.2.4	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	Imprivata FairWarning provides information to customers on the installation of software on select monitored data sources. Customers may use this information to implement controls for these changes.	Full
A.14.2.5	Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	Proper controls are in place in regards to product engineering of the Imprivata FairWarning application, including separation of duties, quality assurance checks and change control.	Full
A.15 Supplier relationships A.15.2 Supplier service delivery management Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.				
A.15.2.1	Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery.	Imprivata FairWarning provides analytics and alerts about access in systems with confidential data. These analytics and alerts include monitoring, reviewing and auditing activity from third parties such as suppliers.	Full
A.15.2.2	Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	Imprivata FairWarning provides analytics and alerts about access in systems with confidential data. These analytics and alerts include monitoring, reviewing and auditing activity from third parties such as suppliers.	Full
A.16 Information security incident management A.16.1 Management of information security incidents and improvements Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.				
A.16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	Imprivata FairWarning's platform provides incident response tracking and management. This assists customers in the prompt and orderly documentation of post-incident analysis, resolution mitigation and other activities.	Full
A.16.1.2	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	Imprivata FairWarning's platform provides incident response tracking and management. This assists customers in the prompt and appropriate reporting of security incidents and their management.	Full

Section	Requirement	Control	Imprivata FairWarning Platform	Imprivata FairWarning Provides Full or Partial Support
A.16.1.3	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	Imprivata FairWarning's platform provides incident response tracking and management. This assists customers in the prompt detection and reporting of any security weaknesses in the areas of user access management and auditing.	Full
A.16.1.4	Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	Imprivata FairWarning's platform provides incident response detection and insight into what caused the incident (i.e., compromised login credentials, elevation of access privileges, etc.). With this information, customers are able to better understand incidents and classify them appropriately.	Full
A.16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Imprivata FairWarning's platform provides incident response tracking and management. This assists customers in assessing how effective (or ineffective) their procedures are and if they align with documented procedures.	Full
A.16.1.6	Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	Imprivata FairWarning's platform provides incident response detection and insight into what caused the incident (i.e., compromised login credentials, elevation of access privileges, etc.). With this information, customers are able to better understand incidents, identify the risks that facilitated the incident, and implement security controls as needed.	Full
A.16.1.7	Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	Imprivata FairWarning's platform provides incident response tracking and management through forensically sound data. In addition, it provides incident response tracking and management via the investigation section allowing for full documentation of post incident analysis, mitigation, and resolution. Customers can use the platform's capabilities to define and implement procedures that enable information to become evidence.	Full
A.18 Compliance A.18.1 Compliance with legal and contractual requirements Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.				
A.18.1.2	Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	Through the use of Imprivata FairWarning's monitoring and alerting, in the areas of user access and auditing, a customer can assess its ongoing compliance. Compliance to protect the customer's IP and proprietary products may be due to legislation, regulations and/or contractual requirements.	Full

Section	Requirement	Control	Imprivata FairWarning Platform	Imprivata FairWarning Provides Full or Partial Support
A.18.1.3	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements.	Imprivata FairWarning's platform enables its customers to monitor confidential data and detect if unauthorized changes, access, release or loss are made to this data. The customer then can apply security controls and protections as needed and demonstrate compliance.	Full
A.18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	Imprivata FairWarning's platform enables its customers to monitor access in systems with confidential data and alert if this access violates security and privacy controls. Because of this, a customer can ensure that the privacy of its PII is maintained and only accessed by those with legitimate need to know.	Full
A.18.2 Information security reviews Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.				
A.18.2.1	Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	Through Imprivata FairWarning's ongoing monitoring and alerting to what confidential data users are accessing, a customer gains insight into the efficacy of their access control policies and processes. This insight can assist the customer in their security efforts related to user access.	Full
A.18.2.2	Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	Through the use of Imprivata FairWarning's monitoring and alerting, a customer can assess its ongoing compliance to standards, like HIPAA, in the areas of user access management and auditing.	Full
A.18.2.3	Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.	Through the use of Imprivata FairWarning's monitoring and alerting, a customer can assess its ongoing compliance to its own internal policies and standards in the areas of user access management and auditing.	Full

*The data above represents a subset of the ISO controls. It only lists those controls where Imprivata FairWarning has full or partial capability to help customers satisfy this control.