MAPPING GUIDE

Mapping to the NHS data security and protection toolkit

What is the Data Security and Protection Toolkit (DSPT) and its purpose?

The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations to measure and publish their performance against the National Data Guardian's ten data security standards. These security standards are clustered under three leadership obligations to ensure:

- People understand how to handle information with respect and care,
- Processes are in place to proactively respond to incidents and prevent data security breaches, and
- Technology is secure and current.

"Leaders of all health and social care organisations should commit to following the data security standards. They should demonstrate this through audit or objective assurance and ensure that audit enables inspection by the relevant regulator." - https://www.dsptoolkit.nhs.uk/Help/Attachment/24

What is the Structure of the DSPT?

The DSPT is composed of ten security standards addressing issues arising from people, processes, and technology. The standards are wide-ranging and cover items ranging from a greater understanding of their security responsibilities among staff to regular reviews of processes to avoid data security breaches to holding information technology (IT) suppliers accountable to protecting confidential data they may access.

With each standard are assertions and these are specific themes or controls that substantiate the standard. Evidence items then follow and represent the maturity of that area.

Fig. 1, an example from the structure

Who must follow the DSPT?

All organisations that have access to NHS patient data and systems must use this toolkit to supply assurances they are practicing thorough data security and that personal information is handled correctly. This mapping guide illustrates how FairWarning can aid Category 1 organisations (i.e., the NHS Trusts) to align with the toolkit.

How does Imprivata FairWarning assist with adherence to the DSPT?

The FairWarning solution focuses on securing the confidential data of its customers within mission critical applications. Use of the FairWarning platform assists customers in either partially or fully fulfilling twenty-three assertions, and forty evidence items within nine (of the ten) data protection standards. FairWarning's solution is a flexible tool that enables customers to show compliance with a variety of assertions. These assertions include prioritisation of top data security risks to proven auditing of those systems holding confidential data to guiding staff security training to achieve a culture of privacy and security.

It is important to note the DSPT is not intended to be a complete data security and protection framework. From NHS Digital - "The standards, assertions, and evidence items are not intended to be a complete framework to manage data security and protection. They represent indicators of good practise and maturity." These good practices and maturities can be part of a larger effort to work towards a security framework such as ISO 27001. FairWarning provides a separate mapping guide illustrating how our solution can aid with fulfillment of that framework's controls.

	Assertion	Evidence Ref	Evidence text – NHS Trusts (Category 1)	Tool Tips – NHS Trust	Imprivata FairWarning Solution	Imprivata FairWarning Managed Privacy Services (MPS)	Full or Partial
Data Protection Standard 1	There is senior ownership of data security and protection within the organisation.	1.1.4	Is data security direction set at board level and translated into effective organisational practices?		Deployment and use of the FairWarning solution demonstrates an organization's commitment to an effective data security and privacy monitoring program for its confidential data. Moreover, the solution provides metrics and reports that educate board members and senior executives on the successes and/or gaps around their data security activities.		Full

	Assertion	Evidence Ref	Evidence text – NHS Trusts (Category 1)	Tool Tips – NHS Trust	Imprivata FairWarning Solution	Imprivata FairWarning Managed Privacy Services (MPS)	Full or Partial
Data Protection Standard 1	There are clear data security and protection policies in place and these are understood by staff and available to the public.	1.2.1	Are there Board approved data security and protection policies in place that follow relevant guidance?	Confirm that you have policies in place that explain the organisation's plan or principles for data protection, data quality, records management, data security, registration authority, Subject access requests, Freedom of Information and network security.	The Imprivata FairWarning solution enables customers to implement data security analytics that continually assess if board approved data security and protection policies are being followed. In addition, an organization's data security values and policies are communicated and reinforced by the investigations, governance and remediation activities supported by the solution.	During onboarding, Imprivata FairWarning MPS analysts will assist the customer in determining if current data security and protection policies align with relevant regulations and guidance. Once the solution is fully deployed, MPS analysts will run the analytics that allow an organization to assess its data protection activities against its policies.	Full
	Individuals' rights are respected and supported. (GDPR Article 12-22)	1.3.4	Provide details of how access to information requests have been complied with during the last twelve months.	Show details of the number of Subject Access Requests and Freedom of Information requests (if relevant) you have received and how many have been responded to on time and how many late.	Imprivata FairWarning helps customers identify what systems contain personal information and other confidential data. During onboarding, Imprivata FairWarning's expertise with data sources assists customers in gaining a more in-depth knowledge of their information assets. With this knowledge, businesses may map out their data assets and respond effectively to verifiable.	Imprivata FairWarning's MPS analysts perform the ongoing monitoring and report building that customer board members use to assess their data security program.	Full

	Assertion	Evidence Ref	Evidence text – NHS Trusts (Category 1)	Tool Tips – NHS Trust	Imprivata FairWarning Solution	Imprivata FairWarning Managed Privacy Services (MPS)	Full or Partial
Data Protection Standard 1	Records of processing activities are documented for all uses and flows of personal information. (GDPR Article 30 and DPA 18 Schedule 1 Part 4)	1.4.1	Provide details of the record or register that details each use or sharing of personal information.	The record should include for each entry: Purpose of processing, Legal basis relied on from GDPR Article 6 and Article 9, Categories of data subject/ personal data, Categories of recipients, whether information is transferred overseas, whether data is retained and disposed of in line with policies, or if not, why not. Whether a written data-sharing agreement or contract is in place and when it ends.	Imprivata FairWarning's solutions assist customers in continually monitoring what information their users are accessing, processing and/or transferring. The solutions give insights into how personal information is being processed within a business and with whom it is being shared.	MPS assists customers in performing the monitoring that details the use, processing, and transfer of information.	Partial
		1.4.3	Provide a list of all systems/ information assets holding or sharing personal information.	This may be your information asset register including details of the: type, location, software, owner, support and maintenance arrangements, quantity of data and how critical they are to the organisation.	Imprivata FairWarning helps customers classify and prioritize their information assets which store personal information and other confidential data. This assistance occurs during onboarding and with addition of data sources by existing customers.	Imprivata FairWarning's MPS team helps customers classify and prioritize their assets (which process personal information and other confidential data) on an ongoing basis.	Partial
	Personal information is used and shared lawfully.	1.5.1	Is there approved staff guidance on confidentiality and data protection issues?	In line with the organisation's data protection policy, there is guidance for staff on using and sharing personal information in accordance with data protection legislation, common law duties, and professional codes and national data opt-out operational policy guidance document, e.g. staff code of conduct, national data opt out model operational policy guidance document and Data Protection Impact Assessment guidance etc.	Usage of the Imprivata FairWarning solution assists customers in communicating to their staff, stakeholders, public and other interested parties that the customer is actively monitoring user access to ensure confidentiality and data protection. This reinforces the guidance to staff that the organization values confidentiality and data protection.		Partial

	Assertion	Evidence Ref	Evidence text – NHS Trusts (Category 1)	Tool Tips – NHS Trust	Imprivata FairWarning Solution	Imprivata FairWarning Managed Privacy Services (MPS)	Full or Partial
Data Protection Standard 1	Personal information is used and shared lawfully.	1.5.2	What actions have been taken following Confidentiality and Data Protection monitoring/spot checks during the last year?	The spot checks should check that staff are doing what it says in your staff Confidentiality and Data Protection guidance and the response should include details of any actions, who has approved the actions and who is taking them forward.	Through use of Imprivata FairWarning's data security and privacy monitoring solution, customers hold their staff and other individuals accessing confidential data accountable. This monitoring can aid in informing and training workforce members.	Imprivata FairWarning's MPS analysts perform the ongoing monitoring and report building that customers use to assess their data security program.	Full
	The use of personal information is subject to data protection by design and by default.	1.6.1	There is an approved procedure that sets out the organisation's approach to data protection by design and by default, which includes pseudonymisation requirements.	The procedures should be approved by the board or equivalent and aim to ensure that only the minimum necessary personal data is processed, that pseudonymisation is used where possible, that processing is transparent allowing individuals to monitor what is being done with their data.	The Imprivata FairWarning solution helps customers support their data protection procedures. With the solution, customers may view and investigate user access to confidential data over multiple applications.	FairWarning's MPS team performs the analytics that assist customers in assessing its data protection procedures. With information from these analytics, customers can assess (and remedy if necessary) its data protection procedures.	Partial
		1.6.2	There are technical controls that prevent information from being inappropriately copied or downloaded.	Technical controls that can support data protection include access control, encryption, computer port control, pseudonymisation techniques etc. Provide details at high level.	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, medical identity or intellectual property theft.	Imprivata FairWarning's 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, medical identity or intellectual property theft.	Partial

	Assertion	Evidence Ref	Evidence text – NHS Trusts (Category 1)	Tool Tips – NHS Trust	Imprivata FairWarning Solution	Imprivata FairWarning Managed Privacy Services (MPS)	Full or Partial
Data Protection Standard 1	There is a clear understanding and management of the identified and significant risks to sensitive information and services.	1.8.2	Senior management have visibility of key risk decisions made throughout the organisation.	Evidence that your board has discussed your top three data security and protection risks and what is being done about them.	The Imprivata FairWarning solution's governance module gives the customer the ability to understand, track, and report on the efficacy of their compliance and data protection efforts. Specifically, the module allows end-users to track metrics from granular detailed reports to high-level trending, can be customized to look at activity from one use/department/facility etc. in the system to all, and can be used to track and report on the status of all investigations into potential inappropriate access and breaches.		Full
		1.8.3	What are your top three data security and protection risks?	Record at a heading level	Imprivata FairWarning's solution provides multiple ways for customers to identify, prioritize and implement risk responses. These include analytics (i.e., enforced policies) to identify use cases indicating inappropriate data access, prioritization of investigations based on those policies, and implementation of governance policies to avoid future reoccurrence of inappropriate data access.	Imprivata FairWarning's MPS team performs the analytics that assist customers in identifying problematic data actions. With that insight, customers determine and prioritize the risk.	Partial

	Assertion	Evidence Ref	Evidence text – NHS Trusts (Category 1)	Tool Tips – NHS Trust	Imprivata FairWarning Solution	Imprivata FairWarning Managed Privacy Services (MPS)	Full or Partial
Data Protection Standard 2	There is a clear understanding of what Personal Confidential Information is held.	2.1.1	The organisation has identified and catalogued personal and sensitive information it holds.	What sensitive information is held or processed and why, where it is held, which systems or services process it and the impact of its loss, compromise or disclosure.	Imprivata FairWarning helps customers classify and prioritize their information assets which store personal information and other confidential data. This assistance occurs during onboarding and with addition of data sources by existing customers.	Imprivata FairWarning's MPS team helps customers classify and prioritize their information assets (which store personal information and other confidential data).	Partial
		2.1.2	When did your organisation last review the list of all systems/ information assets holding or sharing personal information?	The date of the review should be after 1 April 2019. It should be approved by the SIRO or equivalent.	Imprivata FairWarning helps customers classify and prioritize their information assets which store personal information and other confidential data. This assistance occurs during onboarding and with addition of data sources by existing customers.	Imprivata FairWarning's MPS team helps customers classify and prioritize their information assets (which store personal information and other confidential data).	Full
Data Protection Standard 3	There has been an assessment of data security and protection training needs across the organisation.	3.1.1	Has an approved organisation-wide data security and protection training needs analysis been completed after 1 April 2019?	This is an assessment of data security and protection training and development needs for all your staff including Board Members. Approved by your SIRO or equivalent.	Imprivata FairWarning helps customer understand (in depth) the parties accessing, modifying, and/ or transferring their confidential data such as staff and Boarwd Members. With this understanding, customers will have a better assessment of their workforce training needs on data security and protection.	Imprivata FairWarning's MPS team will perform the analytics that help customers understand (in depth) the parties accessing, modifying, and/or transferring their confidential data such as staff and Board Members.	Partial
	Staff with specialist roles receive data security and protection training suitable to their role.	3.3.1	Provide details of any specialist data security and protection training undertaken.	Details of any additional training as identified by your Data Security Training Needs analysis. Such as staff with roles in Informatics (IT and Information areas), Medical Records, Clinical Coding & Information Governance (including privacy / confidentiality & data protection).	Imprivata FairWarning helps customer understand (in depth) the parties accessing, modifying, and/ or transferring their confidential data such as those in specialist roles. With this understanding, customers will have a better assessment of their workforce training needs on data security and protection.	Imprivata FairWarning's MPS team will perform the analytics that help customers understand (in depth) the parties accessing, modifying, and/or transferring their confidential data such as those in specialist roles.	Partial

	Assertion	Evidence Ref	Evidence text – NHS Trusts (Category 1)	Tool Tips – NHS Trust	Imprivata FairWarning Solution	Imprivata FairWarning Managed Privacy Services (MPS)	Full or Partial
Data Protection Standard 4	The organisation maintains a current record of staff and their roles.	4.1.2	Does the organisation understand who has access to personal and confidential data through your systems, including any systems which do not support individual logins?	Each system may use its own user list(s) or use federated access. There may be systems where technically or operationally it is not possible to have individual logins but there are alternative methods of maintaining user lists. Where this occurs, it is understood and risk assessed by the organisation.	Imprivata FairWarning helps customer understand (in depth) the parties accessing, modifying, and/or transferring their confidential data such as employees, contractors, partners etc. In addition, the FairWarning solution leverages our patented Dynamic Identity Intelligence to further help customers identify those accounts accessing personal and confidential data. Dynamic Identity Intelligence correlates user information from all of a care provider's data sources (example - Active Directory, HR Systems, EHRs). This centralization more accurate information available about a user (than from single data sources).	Imprivata FairWarning's MPS team will perform the analytics that help customers understand (in depth) the parties accessing, modifying, and/or transferring their confidential information.	Full
		4.1.3	Are users in your organisation only given the minimum access to sensitive information or systems necessary for their role?		Imprivata FairWarning helps customers identify what confidential data their users are accessing. With this insight, customers can continually assess and manage the access permissions and authorizations of those users.	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.	Full
	Organisation assures good management and maintenance of identity and access control for it's networks and information systems.	4.2.1	When was the last audit of user accounts held?	An audit of staff accounts from your organisation, to make sure there aren't any inappropriate access permissions. Record the date when the last user audit was held. This should be completed annually as a minimum.	Use of the Imprivata FairWarning solution provides an ongoing monitoring and auditing of user accounts. The solution provides automated alerts that will indicate inappropriate access permissions.		Partial

	Assertion	Evidence Ref	Evidence text – NHS Trusts (Category 1)	Tool Tips – NHS Trust	Imprivata FairWarning Solution	Imprivata FairWarning Managed Privacy Services (MPS)	Full or Partial
Data Protection Standard 4	Organisation assures good management and maintenance of identity and access control for it's networks and information systems.	4.2.2	Provide a summary of data security incidents in the last 12 months caused by a mismatch between user role and system accesses granted.	This can be an incident either where the staff member's rights to data was too high or too low. Do not name individuals.	Imprivata FairWarning's solution provides monitoring for potential data breaches, incident response tracking and management. This assists customers in the prompt and orderly documentation of data security incidents, post incident analysis, resolution mitigation and other activities.	Imprivata FairWarning's MPS team acts as an extension of the customer's incident response team by identifying and documenting incident occurrence, post incident analysis, resolution mitigation and other activities.	Partial
		4.2.5	Are unnecessary user accounts removed or disabled?	Internal workstations (or equivalent Active Directory domain) (e.g. Guest, previous employees) removed or disabled.	Imprivata FairWarning's solution does not provision or de-provision user identities or credentials . However, FairWarning can identify users who are accessing confidential data but their employment status is no longer valid.	Imprivata FairWarning's MPS team will perform analytics that can detect access by unnecessary user accounts.	Full
	All staff understand that their activities on IT systems will be monitored and recorded for security purposes.	4.3.4	Provide a list of all systems to which users and administrators have an account, plus the means of monitoring access.	For each system holding personal data that support users and administrative accounts, how user access is monitored should be recorded. If it is not monitored then this should be recorded.	Imprivata FairWarning helps customers classify and prioritize their information assets which store ePHI and other confidential data. This assistance occurs during onboarding and with addition of data sources by existing customers. Imprivata FairWarning's solution prduces comprehensive monitoring for all user and 3rd party activity in confidential data containing applications the customer chooses to monitor. The use of the solution helps customers to understand the data actions around their confidential data (i.e., who/what/when/where of data accessed). With this knowledge, customers can provide protection for confidential data and remediate any vulnerability gaps in its data protection efforts.	Imprivata FairWarning's MPS team performs the comprehensive monitoring that helps customers understand the user and administrator access into their systems.	Full

	Assertion	Evidence Ref	Evidence text – NHS Trusts (Category 1)	Tool Tips – NHS Trust	Imprivata FairWarning Solution	Imprivata FairWarning Managed Privacy Services (MPS)	Full or Partial
Data Protection Standard 4	All staff understand that their activities on IT systems will be monitored and recorded for security purposes.	4.3.5	Have all staff been notified that their system use could be monitored?	Staff are informed and understand that their system can be monitored and recorded. The notification method is periodic.	Usage of the Imprivata FairWarning solution assists customers in communicating to their staff, stakeholders, public and other interested parties the importance of privacy to the customer and its data protection efforts.. A data protection program, which is supported by the solution, reinforces the message that organization values privacy and data protection.		Partial
	You closely manage privileged user access to networks and information systems supporting the essential service.	4.4.1	Has the Head of IT, or equivalent, confirmed that IT administrator activities are logged and those logs are only accessible to appropriate personnel?	IT Support staff typically have high level access to systems. The activities of these users should be logged and only available to appropriate personnel. If no systems select Yes.	With the Imprivata FairWarning solution, IT Heads can track what data their staff are accessing and assess if this access is appropriate or not. With this insight, IT Heads can ensure that IT Support Staff are engaged in appropriate access only.	Imprivata FairWarning's MPS team will perform analytics that can detect inappropriate access among IT Support Staff.	Partial
		4.4.2	Privileged user access is removed when no longer required or appropriate.	Provide details of access reviews in the last twelve months.	Imprivata FairWarning's solution does not provision or de-provision user identities or credentials . However, using the solution's Dynamic Identity Intelligence, FairWarning can identify users who are accessing confidential data but their employment status is no longer required (i.e., as in the case of job change) or valid (as in the case of job termination).	Imprivata FairWarning's MPS team will perform analytics that can detect access by staff that is no longer required or appropriate.	Partial
	You ensure your passwords are suitable for the information you are protecting.	4.5.5	Does your organisation grant limited privileged access and third party access for a limited time period or is planning to?		Without a monitoring solution determining what data their third parties are accessing (and how often), an organization is not holding anyone accountable to their limited and time sensitive access. Use of the FairWarning solution enforces those limits.	Imprivata FairWarning's MPS analysts run the ongoing analytics that assess privileged and third party access.	Partial

	Assertion	Evidence Ref	Evidence text – NHS Trusts (Category 1)	Tool Tips – NHS Trust	Imprivata FairWarning Solution	Imprivata FairWarning Managed Privacy Services (MPS)	Full or Partial
Data Protection Standard 5	Process reviews are held at least once per year where data security is put at risk and following data security incidents.	5.1.1	Root cause analysis is conducted routinely as a key part of your lessons learned activities following a data security incident.	To cover data security and protection incidents.	Imprivata FairWarning's solution enables customers to investigate potential data security incidents and their underlying root causes. It does so by assessing users and their behaviours to identify root causes such as insiders with excess access permissions, or weak deprovisioning procedures that allow for access after employee termination. This insight assists customers in the prompt and orderly documentation of post incident analysis, resolution mitigation and other activities.	Imprivata FairWarning's MPS team acts as an extension of the customer's incident response team by identifying and documenting incidents, their root causes and mitigation.	Partial
	Process reviews are held at least once per year where data security is put at risk and following data security incidents.	5.1.2	Provide summary details of process reviews held to identify and manage problem processes which cause security breaches.	Processes which have caused breaches or near misses, are reviewed to identify and improve processes which force staff to use workarounds which compromise data security.	Imprivata FairWarning's solution enables customers to investigate potential data security incidents and their underlying workflows. It does so by assessing users and their behaviours to workarounds that compromise data security such as users sharing login credentials. This insight assists customers in the prompt and orderly documentation of post incident analysis, resolution mitigation and other activities.	Imprivata FairWarning's MPS team acts as an extension of the customer's incident response team by identifying and documenting problematic workarounds.	Partial
	Action is taken to address problem processes as a result of feedback at meetings or in year.	5.3.2	Post testing findings should inform the immediate future technical protection of the system or service, to ensure identified issues cannot arise in the same way again.	Explain how any incident response and management tests findings have informed the immediate future technical protection of the system or service, to ensure identified issues cannot arise in the same way again.	Usage of Imprivata FairWarning's full lifecycle privacy management solution provides customers ability to respond to inappropriate access incidents at multiple stages including identification, analysis and response. Customers may respond to access incidents identified within the solution and/or document and track problematic data actions learned of from researchers, professional events or other sources.	Imprivata FairWarning's MPS team performs the analytics that assist customers in identifying inappropriate access incidents. With that insight and findings, customers can change processes to prevent those incidents from reoccurring.	Full

	Assertion	Evidence Ref	Evidence text – NHS Trusts (Category 1)	Tool Tips – NHS Trust	Imprivata FairWarning Solution	Imprivata FairWarning Managed Privacy Services (MPS)	Full or Partial
Data Protection Standard 5	Action is taken to address problem processes as a result of feedback at meetings or in year.	5.3.3	Systemic vulnerabilities identified in process reviews shall be remediated as soon as practicable.	Explain how any Systemic vulnerabilities are remediated.	Imprivata FairWarning's solution produces comprehensive monitoring for all user and 3rd party activity in confidential data containing applications the customer chooses to monitor. The use of the solution helps customers to understand the access issues around their confidential data (i.e., who/what/when/where of data accessed). With this knowledge, customers can provide protection for confidential data and remediate any vulnerability gaps in its data protection efforts.	Imprivata FairWarning's MPS team performs the analytics that assist customers in identifying inappropriate access incidents. With that insight and findings, customers can change processes to prevent those incidents from reoccurring.	Partial
Data Protection Standard 6	A confidential system for reporting data security and protection breaches and near misses is in place and actively used.	6.1.1	A data security and protection breach reporting system is in place.	Confirmation that a functioning data security and protection breach reporting mechanism is in place including use of the DSP Toolkit Incident reporting tool.	Imprivata FairWarning's solution provides monitoring for potential data breaches, incident response tracking and management. This assists customers in the prompt and orderly documentation of post incident analysis, resolution mitigation and other activities.	Imprivata FairWarning's MPS team acts as an extension of the customer's incident response team by identifying and documenting risks and their mitigation.	Partial
	Known vulnerabilities are acted on based on advice from CareCERT, and lessons are learned from previous incidents and near misses.	6.3.1	If you have had a data security incident, was it caused by a known vulnerability?	Provide details of incidents over the reporting period (a year). Known vulnerabilities are those listed on the CareCERT portal, if viewable. If no incidents have occurred mark None.	Imprivata FairWarning's solution produces comprehensive monitoring for all user and 3rd party activity in confidential data containing applications the customer chooses to monitor. The use of the solution helps customers to understand the data actions around their confidential data (i.e., who/what/when/where of data accessed). With this knowledge, customers can provide protection for confidential data and remediate any vulnerability gaps in its data protection efforts.	Imprivata FairWarning's MPS team performs the analytics that assist customers in identifying inappropriate access incidents. With that insight and findings, customers can change processes to prevent those incidents from reoccurring.	Partial

	Assertion	Evidence Ref	Evidence text – NHS Trusts (Category 1)	Tool Tips – NHS Trust	Imprivata FairWarning Solution	Imprivata FairWarning Managed Privacy Services (MPS)	Full or Partial
Data Protection Standard 6	Known vulnerabilities are acted on based on advice from CareCERT, and lessons are learned from previous incidents and near misses.	6.3.3	The Organisation has a proportionate monitoring solution to detect cyber events on systems and services.	Includes an assessment of all systems monitoring requirements.	Imprivata FairWarning's solution produces comprehensive monitoring for all user and 3rd party activity in confidential data containing applications the customer chooses to monitor. The use of the solution helps customers to understand the events around their confidential data (i.e., who/what/when/where of data accessed).	Imprivata Imprivata FairWarning's MPS team performs the comprehensive monitoring to detect cyber events.	Full
		6.3.5	Are all new Digital services that are attractive to cyber criminals for the purposes of fraud, implementing transactional monitoring techniques from the outset?	Includes an assessment of which services are susceptible to fraud, if none respond 'Yes' and explain in the comments section.	Imprivata FairWarning helps customers monitor and investigate inappropriate access to ePHI and other confidential data. With this assistance, customers can be protected from fraudulent activities such as identity, medical identity or intellectual property theft.	Imprivata FairWarning's MPS staff monitors and investigates inappropriate access to customer ePHI and other confidential data. With this assistance, customers can be protected from fraudulent attempts such as identity, medical identity or intellectual property theft.	Partial
		6.3.6	Have you had any repeat data security incidents of the same issue within the organisation?	A repeat incident is defined as an exploitation of the same vulnerability on the same systems or different ones, that occurs within 3 calendar months of the original or subsequent occurrences. Provide details.	Usage of the Imprivata FairWarning solution gives customers insight into whether their data protection processes are working or not. With this understanding of how and where their data protection efforts are weak and/or absent, a customer can improve its data protection processes.	Imprivata FairWarning's MPS staff monitors and investigates inappropriate access to a customer's confidential data. With this assistance, customers can assess its data protection processes and apply changes and/or mitigating controls as needed.	Partial

	Assertion	Evidence Ref	Evidence text – NHS Trusts (Category 1)	Tool Tips – NHS Trust	Imprivata FairWarning Solution	Imprivata FairWarning Managed Privacy Services (MPS)	Full or Partial
Data Protection Standard 7	You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions.	7.3.1	On discovery of an incident, mitigating measures shall be assessed and applied at the earliest opportunity, drawing on expert advice where necessary.	From NHS Digital or a Cyber Incident Response (CIR) company	Imprivata FairWarning's solution provides monitoring for potential data breaches, incident response tracking and management. This assists customers in the prompt and orderly response to an incident, documentation of post incident analysis, resolution mitigation and other activities.	Imprivata FairWarning's MPS team acts as an extension of the customer's incident response team by identifying and documenting risks and their mitigation.	Partial
Data Protection Standard 9	You have demonstrable confidence in the effectiveness of the security of your technology, people, and processes relevant to essential services.	9.4.1	You validate that the security measures in place to protect the networks and information systems are effective, and remain effective for the lifetime over which they are needed.	Please provide an explanation.	Through use of the Imprivata FairWarning solutions, customers are implementing controls that can assess the effectiveness (or not) of security procedures. Procedure examples include when deprovisioning of a terminated user does not occur and that user maintains access to confidential data or when a user has access to confidential data without a legitimate need-to-know. With that knowledge, customers may strengthen their user account management procedures.		Partial

	Assertion	Evidence Ref	Evidence text – NHS Trusts (Category 1)	Tool Tips – NHS Trust	Imprivata FairWarning Solution	Imprivata FairWarning Managed Privacy Services (MPS)	Full or Partial
Data Protection Standard 9	You have demonstrable confidence in the effectiveness of the security of your technology, people, and processes relevant to essential services.	9.4.4	Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way.		Usage of Imprivata FairWarning's full lifecycle privacy management solution assists customers with security deficiencies at multiple stages including identification, analysis and response. Customers can then respond to deficiencies identified within the solution and investigate, prioritize and remedy as necessary.		Partial
Data Protection Standard 10	Basic due diligence has been undertaken against each supplier that handles personal information in accordance with ICO and NHS Digital guidance.	10.2.4	Where services are outsourced (for example by use of cloud infrastructure or services), the organisation understands and accurately records which security related responsibilities remain with the organisation and which are the supplier's responsibility.		Without a monitoring solution determining what data their third parties are accessing, an organization is not holding anyone accountable to their roles and responsibilities with respect to data security. Use of the FairWarning solution enforces the establishment of those responsibilities.		Partial

	Assertion	Evidence Ref	Evidence text – NHS Trusts (Category 1)	Tool Tips – NHS Trust	Imprivata FairWarning Solution	Imprivata FairWarning Managed Privacy Services (MPS)	Full or Partial
Data Protection Standard 10	The organisation understands and manages security risks to networks and information systems from your supply chain.	10.5.1	Your organisation's approach to risk management includes the risks to your services arising from supply chain.		Imprivata FairWarning's solution enables comprehensive monitoring for all user and third party activity to confidential data in applications the customer chooses to monitor. The use of the solution helps customers to understand any data access issues arising from their third party partners. (i.e., who/what/when/ where of data accessed). With this knowledge, customers can provide protection for confidential data and remediate any vulnerability gaps in its data protection efforts introduced by third parties.	Imprivata FairWarning's MPS team performs the comprehensive monitoring that helps customers understand the access issues introduced by third parties.	Partial
		10.5.2	Where appropriate, you offer support to suppliers to resolve incidents.		With the Imprivata FairWarning solution, third parties can be educated on what data their staff are accessing and if this access is appropriate or not. With this insight, they have a better understanding of their roles and responsibilities.		Partial