Statement of HIPAA and GDPR Compliance

As a leading provider of X-ray medical imaging devices, Adaptix is committed to ensuring the privacy and security of Private Health Information (PHI) in compliance with the US Health Insurance Portability and Accountability Act (HIPAA), the relevant sections of the UK Data Protection Act 2018, incorporating the specific UK General Data Protection Regulation (GDPR) Article 6, pertaining to PHI. Our commitment to complying with these is demonstrated through the following practices:

1. **No Intent to Collect, Process, nor Store PHI**: Adaptix does not store any PHI on its servers or any other company property. Our X-ray devices are designed to operate independently of Adaptix, and with the medical organisation's (or third party) Radiology Information System (RIS) and the Picture Archiving and Communication System (PACS). This ensures that PHI remains within the medical organisations that utilise our equipment.

2. **Service & Support protocols**: during service and support activities, Adaptix employees and engineers providing service and support may encounter PHI stored on the device. In such instances, our relevant employees are trained to handle PHI with the utmost confidentiality and in strict adherence to HIPAA regulations. They are required to follow established protocols to ensure that PHI is not disclosed, accessed, or used inappropriately. These protocols are set out in Annex A [where this is an Annex to this document with the intent that the statement will be published on our website and the Annexes will not be published but appropriately stored as referenced QMS documents].

3. **Safeguards:** Adaptix has established business systems, policies and cyber security with technical and physical safeguards to comprehensively prevent (in line with FDA 510(k) pre-market submission requirements) any data or information (including any PHI) from being intentionally or unintentionally used or disclosed in violation of HIPAA's requirements. Technical safeguards include limiting access to information by creating computer firewalls. Physical safeguards include tamper-proof screws on the device used by our clients, as well as locking doors or filing cabinets and periodically changing door access codes in all Adaptix buildings. Additionally, all staff members can only access relevant information (including PHI, where relevant) by using their own login information. Firewalls ensure that only authorised employees will have access to PHI, that they will have access to only the minimum amount of PHI necessary for their job functions, and that they will not further use or disclose PHI in violation of HIPAA's privacy rules.

4. **Employee Training**: all relevant Adaptix employees involved in service and support, undergo comprehensive HIPAA training. This training includes understanding the importance of PHI, recognising potential risks, and implementing best practices to safeguard patient information. This training is detailed in Annex B.
5. **Confidentiality Agreements**: Adaptix requires all employees to sign confidentiality agreements that explicitly outline their responsibilities in protecting all company data that is sensitive, which includes intellectual property, personal and confidential and private personal data and also private health information of any third-party person or organisation. This is captured and referred to in a term, "Confidential Information" which is explained and agreed to by the signee [employee]. These agreements reinforce our commitment to maintaining the privacy and security of patient information.

6. **Incident Response**: in the unlikely event of a PHI breach, Adaptix will respond to this in line with our incident response plan set out in Annex C of this document. This is to promptly

address and mitigate any potential risks. This plan includes notifying affected parties and taking corrective actions to prevent future occurrences.

Adaptix is dedicated to maintaining the highest standards of privacy and security for PHI, ensuring that our clients can trust us with their sensitive information. Our adherence to HIPAA and other relevant national data protection regulations reflects our commitment to protecting patient privacy and supporting the global healthcare community.

For any questions or further information regarding our HIPAA compliance practices, please contact our Quality & Regulatory team.

ANNEX A: Service & Support Protocols

1. **Access Control**: service engineers must only access PHI when absolutely necessary for performing their duties and access will be limited to the minimum necessary information (per section 164.514(d) of the HIPAA Privacy Rule and UK GDPR).
2. **Confidentiality**: engineers must maintain the confidentiality of any PHI they encounter during service activities. They should avoid discussing PHI in public or unsecured areas (per section 164.530(c) of the HIPAA Privacy Rule).
3. **Transparency:** Adaptix must inform clients about the potential for service engineers to access PHI and the measures taken to protect it.
4. **Secure Handling**: any PHI viewed during service must be handled securely. This includes ensuring that electronic devices are password-protected and that any written notes are securely stored or destroyed (per section 164.312(a) of the HIPAA Security Rule).
5. **Documentation**: service activities involving PHI must be documented, including the purpose of access and the specific information accessed. This documentation helps ensure accountability and traceability (per section 164.312(b) of the HIPAA Security Rule).
6. **Legitimate Interest**: while Adaptix has no intent of processing any PHI, if it necessary to process X-ray images which contain PHI, this will only be carried out for the legitimate interests of the individual PHI owner, medical organisation or a third party, unless overridden by the individual's data protection rights (per UK GDPR Article 6).
7. **Purpose Limitation**: data will only be seen during service and support for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
8. **Integrity and Confidentiality**: all our data (permanent and temporary) is be processed in a manner that ensures appropriate security, per the Adaptix Medical Device Security Policy (per UK GDPR Article 6).
9. **Storage Limitation**:

    a. whereby X-ray images are processed as part of this specific, explicit and legitimate service and support (which might contain PHI), this will be processed in this specific manner to debug and resolve customer issues only (per point (f) above), and if that means storing and data, this will be deleted upon resolution of the service to the customer, and no longer than necessary.
    b. For the sake of service and support by Adaptix (if a customer has a complaint about certain X-ray images they have captured), the device stores the most recent images up to a set amount. These most recent ones are captured with older ones being deleted; hence they are kept in a form that permits identification of data subjects for no longer than necessary. They are more permanently stored by the client, independent of Adaptix (per UK GDPR Article 6).

10. **Data Minimisation**: data must be adequate, relevant, and limited to what is necessary.
11. **Accuracy**: data must be accurate and kept up to date.
12. **Storage Limitation**: data must be kept in a form that permits identification of data subjects for no longer than necessary.
13. **Integrity and Confidentiality**: data must be processed in a manner that ensures appropriate security.

ANNEX B: Training Elements for Service & Support Staff

1. **Initial Training**: all new employees working in service and support receive training on HIPAA policies and procedures as they relate to their specific roles, as well as understanding the lawful bases for processing personal data under Article 6 of the UK GDPR, and the principles of data protection as outlined in the UK Data Protection Act 2018. This training must occur within a reasonable period after the employee joins the organisation (per section 164.530(b)(1) of the HIPAA Privacy Rule). This reasonable period is 30 days.
2. **Ongoing Training**: employees receive periodic refresher training to updated on any changes to HIPAA regulations and organisational policies (per section 164.308(a)(5) of the HIPAA Security Rule).
3. **Security Awareness**: training includes security awareness and best practices for protecting PHI, per our cyber security policies and protocols, such as recognising phishing attempts, using strong passwords, and securing electronic devices (per section 164.308(a)(5) of the HIPAA Security Rule).
4. **Incident Reporting**: employees are trained on how to report potential security incidents or breaches involving PHI (per section 164.314(a)(2)(i) of the HIPAA Security Rule).

ANNEX C: Incident Response Plan for HIPAA Compliance

Objective: to promptly address and mitigate potential risks associated with breaches of Private Health Information (PHI), ensuring compliance with HIPAA and UK Data Protection regulations. Below is an incident response plan specifically for PHI, but Adaptix also has wider company Security Incident Handling and Response Plan (DMS-14890). This latter, broader document carries the ultimate authority (if a PHI incident overlaps with it being a Security breach), which more comprehensively assessing response times, urgency and criticality (unless HIPAA requirements are breached – in this case, the lower response time will typically be adhered to).

1. Detection and Reporting

Step 1: Identification

- **Action**: Identify potential security incidents through monitoring systems, employee reports, or external notifications.
- **Timeline**: Immediate upon detection.

Step 2: Initial Reporting

- **Action**: Report the incident to a designated Incident Response Team (IRT) who will be made of the appropriate personnel (on a case-by-case basis) of our wider Security Risk Management Team, as well as personnel from the Senior Leadership Team; this will be the same team for reporting cyber security incidents.
- **Timeline**: Within 24 hours of detection.

2. Assessment and Classification

Step 3: Incident Classification

- **Action**: Assess the severity of the incident based on the type and amount of PHI involved, the potential impact on individuals, and the likelihood of harm.

- **Severity Levels**
    - **Low**: Minimal PHI involved, low risk of harm.
    - **Medium**: Moderate amount of PHI involved, potential risk of harm.
    - **High**: Significant amount of PHI involved, high risk of harm.
- **Timeline**: Within 48 hours of initial reporting.

3. Containment and Mitigation

Step 4: Immediate Containment

- **Action**: Implement measures to contain the incident and prevent further unauthorized access or disclosure.
- **Timeline**: Within 24 hours of classification.

Step 5: Mitigation

- **Action**: Mitigate the harmful effects of the incident to the extent practicable, such as securing affected systems and removing unauthorized access.
- **Timeline**: Within 72 hours of classification.

4. Notification

Step 6: Notification of Affected Parties

- **Action**: Notify individuals whose PHI has been compromised. The notification should include a description of the incident, the types of PHI involved, steps individuals should take to protect themselves, and what the organization is doing to investigate and mitigate the breach.
- **Timeline**: Within 60 days of discovering the breach (per section 164.404 of the HIPAA Breach Notification Rule). NOTE (per UK GDPR): Adaptix will notify affected individuals without undue delay if the breach is likely to result in a high risk to their rights and freedoms.

Step 7: Notification of Regulatory Bodies

- **Action**: Notify the US Department of Health and Human Services (HHS) and, if applicable, the media for breaches affecting more than 500 individuals.
- **Timeline**: Within 60 days of discovering the breach for large breaches; annually for breaches affecting fewer than 500 individuals (per section 164.408 of the HIPAA Breach Notification Rule). NOTE (per UK GDPR): Iin the event of a data breach that is likely to result in a risk to the rights and freedoms of individuals., Adaptix will notify the UK Information Commissioner's Office (ICO) within 72 hours.

5. Investigation and Documentation

Step 8: Investigation:

- **Action**: Conduct a thorough investigation to determine the cause of the incident and identify any vulnerabilities.

- **Timeline**: Ongoing, with a preliminary report within 30 days.

Step 9: Documentation:

- **Action**: Document all facts relating to, and actions taken in response to, any incidents or breaches, including detection, impacts, reporting, classification, containment, remedial action, mitigation, and notifications.
- **Timeline**: Ongoing, with a final report within 60 days.

6. Corrective Actions and Prevention

Step 10: Corrective Actions:

- **Action**: Implement corrective actions to address identified vulnerabilities and prevent future occurrences. This may include updating policies, enhancing security measures, and providing additional employee training.
- **Timeline**: Within 90 days of the final report.

Step 11: Review and Improvement:

- **Action**: Review the incident response process and make improvements based on lessons learned.
- **Timeline**: Annually or after each significant incident.

By following this incident response plan, Adaptix ensures that any breaches of PHI are promptly addressed and mitigated, in compliance with HIPAA regulations. This plan helps protect patient privacy and maintain trust with our clients and the US and global healthcare community.