Body Worn Video

Privacy Impact Assessment

May 2019

Aspects of Privacy Impact Assessment

There are four aspects of privacy to be considered when undertaking a PIA, they will at times overlap and should be seen as working guides to the issues a PIA should explore, rather than strict definitions.

A PIA should consider:

1. The privacy of personal information;
   This aspect is referred to variously as 'data privacy' and 'information privacy'. Individuals generally do not want data about themselves to be automatically available to other individuals and organisations. Even where data is possessed by another party, the individual should be able to exercise a substantial degree of control over that data and its use. The development of information technologies have had substantial impacts on information privacy.
2. The privacy of the person;
   This aspect is sometimes referred to as 'bodily privacy', and is concerned with the integrity of the individual's body. Issues associated with privacy include body searches, compulsory immunisation, blood transfusion without consent, compulsory provision of samples of body fluids and body tissue, and requirements for submission to biometric measurement.
3. The privacy of personal behaviour;
   This aspect relates to the observation of what individuals do, and includes such issues as optical surveillance and 'media privacy'. It could relate to matters such as sexual preferences and habits, political or trade union activities and religious practices. But the notion of 'private space' is vital to all aspects of behaviour, it is relevant in 'private places' such as the home and toilet cubicle, and is also relevant in 'public places', where casual observation by the few people in the vicinity is very different from systematic observation, the recording or transmission of images and sounds.
4. The privacy of personal communications.
   This aspect could include various means of analysing or recording communications such as mail 'covers', the use of directional microphones and 'bugs' with or without recording apparatus and telephonic interception and recording. In recent years, concerns have arisen about third party access to email messages. Individuals generally desire the freedom to communicate among themselves, using various media, without routine monitoring of their communications by other persons or organisations.

Privacy Impact Assessment Proforma

This document must be completed for any new / or change in service which pertains to utilise personal identifiable information. It must be completed as soon as the new service / or change is identified by the Project Manger / System Manager or Information Asset Owner.

This process is a mandated requirement on the Information Governance Toolkit to ensure that privacy concerns have been considered and actioned to ensure the security and confidentiality of the personal identifiable information.

There are 2 types of Privacy Impact Assessments – a small scale and full scale. This proforma is based on the Small Scale PIA. Following completion of this proforma, it may be necessary to conduct a Full Scale PIA. Full details are available in the Information Commissioner‟s handbook.
Privacy Law compliance checks and General Data Protection Regulation compliance checks are part of the PIA process – the questions to assess this are included in the proforma.
Please complete all questions with as much detail as possible and return the completed form to:

Information Governance
Information.governance@nhs.net

Further guidance on specific items can be found on the Information Commissioner‟s website.
www.ico.gov.uk

Section A: New Project Details

Name: Body Worn Video – Security Officers

Objective: The project aim is to

- To protect staff, patients and visitors
- To protect Trust premises and Trust assets
- To increase personal safety and reduce the fear of crime
- To reduce incidents of violence and aggression to staff members
- To support the Police in reducing and detecting crime
- To assist in identifying, apprehending and prosecuting offenders
- To provide a deterrent effect and reduce criminal activity
- To assist in the traffic management and car parking schemes

Background: Body Worn Video (BVW) equipment consists of a small camera attached to the uniform of security officers which record visual and sound data by the officers during tours of duty. The purpose of the recording is to safeguard staff, patients and the officers during violent and aggressive or anti-social behaviour incidents. The footage will be in an encrypted format, securely stored and only viewed by authorised persons. The devices will only be activated during an incident and continuous recording is strictly not permitted.

Benefits: Are:

- Protection of all staff
- Deterrent and encourages compliance through self-awareness
- Supports de-escalation of violence
- Safety of staff by reducing verbal and physical attacks
- Contribute to the transparency of security procedures
- Provision of verifiable recordings with time-stamp & support statements
- Saving lengthy descriptive reports having to be provided
- Footage is readily acceptable by courts and CPS
- Acceleration of judicial process by encouraging early guilty pleas
- A reduction in complaints against staff
- BWV should reduce absenteeism by supporting with all the above
- A tangible contribution to efficient work flow and cost savings

Constraints:

- Entitlement to footage, possible release to third parties
- Possible additional costs for data storage
- Recording & handling sensitive footage
- BWV must be worn and carried
- Continuity of evidence
- Battery life

Relationships: (for example, with other Trust's, organisations)

Networking information with other Trusts that have deployed BWV, Leeds, Goole and Doncaster.
Improved relationships with police and Crown Prosecution Service – evidence retention.
Relationship with ambulance service – violence & aggression incidents.
Local Authority – parking enforcement, smoking, litter, dog fouling on site
Fire Service – Fire prevention and reduction.

Quality expectations:

- Reduction in anti-social behaviour
- Reduction in incidents of violence & aggression
- Reduction in complaints
- Staff security & safety perceptions
- Deterrent measures
- Savings in sickness absence
- Improvements in evidence data

Cross reference to other projects: Trust CCTV system

Project Manager: Mike Lees

Name: Mike Lees	Name: Lisa Corbridge
Title: Head of Business Security	Title: Business Security Specialist
Department: BSU	Department: BSU
Telephone: 01226 431386	Telephone: 01226 431387
Email: mike.lees@nhs.net	Email: lisacorbridge@nhs.net

Information Asset Owner: (All systems/assets must have an Information Asset Owner (IAO). IAO's are normally the Heads of Departments and report to the SIRO)

Name: Mike Lees
Title: Head of Business Security
Department: Business Security Unit
Telephone: 01226 431386
Email: mike.lees@nhs.net

Customers and stakeholders:
Name:

- Business Security Unit
- Trust Security Team
- G4S Security Services
- Barnsley Facilities Services (BFS)
- All Trust staff including volunteers, non-executive directors and governing body
- Trust Members
- Trust Service Users (Patients, Visitors, Relatives)
- All staff side organisations
- Human Resources Department
- W.H. Smith Ltd
- Barnsley Hospital Charity
- Contracted staff and service providers
- NHS Barnsley Clinical Commissioning Group
- NHS England
- South Yorkshire Police
- Yorkshire Ambulance Service
- South Yorkshire Fire & Rescue Services
- Barnsley Metropolitan Borough Council including elected members
- South West Yorkshire NHS Foundation Trust
- Care UK
- NHS Professionals
- Pogmoor & Old Town Residents

Section B Privacy Impact Assessment Key Questions

Question	**Response**		Ref to key req. e.g. IGTK, Small scale PIA etc
1. Will the system (will now be referred to thereafter as 'asset') contain Personal Identifiable Data or Sensitive Data? If answered 'No' you do not need to complete any further information as PIA is not required.	Patients Visitors Relatives Staff Contractors		
2. Please state purpose for the collection of the data: for example, patient treatment, health administration, research, audit, staff administration	• To protect staff, patients and visitors • To protect Trust premises and Trust assets • To increase personal safety and reduce the fear of crime • To reduce incidents of violence and aggression to staff members • To support the Police in reducing and detecting crime • To assist in identifying, apprehending and prosecuting offenders • To provide a deterrent effect and reduce criminal activity • To assist in the traffic management and car parking schemes		IGTK 202
3. Does the asset involve new privacy–invasive technologies?	Yes If yes, please give details:		SS PIA (1)
4. Please tick the data items that are held in the system	**Personal** Name Photographic/Video footage Voice audio	**Sensitive**	
5. Will the asset collect new personal data items which have not been collected before?	Yes Audio/Sound data		SS PIA (5)
6. What checks have been made regarding the adequacy, relevance and necessity for the	Security Officers only deploy BWV technology against the defined operational requirements and Security Policy and ensure that the use is		SS PIA (2 & 10)

collection of personal and/or sensitive data for this asset?	proportionate, legitimate, necessary and justifiable. In addition, it will ensure that the use satisfies the requirement of addressing a pressing staff and patient safety need described in Trust policy, the assignment instructions and NHS security management advice and guidance. At all stages it will comply with the General Data Protection Regulation and other legislation. In the case of the Human Rights Act 1998, there will be adherence to the requirements of Article 6 (Right to a fair trial) and in respect of Article 8 (Right to respect for private and family life, home and correspondence) since this is a qualified right, information will only be captured and processed to achieve a legitimate aim as detailed earlier.	
7. Does the asset involve new or changed data collection policies that may be unclear or intrusive?	No Previous versions of the Trust CCTV policy have included the procedures and processes for data collection and have been subject of full consultation and approval by Trust Board. The CCTV policy has been recently revised to include BWV and renamed to the Surveillance Camera Policy.	SS PIA (9)
8. Is the third party contract/supplier of the system registered with the Information Commissioner? What is their notification number?	Yes G4S Security Solutions UK – Z7118067 Reveal Media Ltd – ZA089885	
9. Does the third party/supplier contracts contain all the necessary Information Governance clauses including information about Data Protection and Freedom of Information?	Yes Contract renewed 1st April 2016	IG TK 110
10. Does the asset comply with privacy laws such as the Privacy and Electronic Communications Regulation 2003 (see appendix for definition)	Yes	Privacy Law Check
11. Who provides the information for the asset?	Patient Staff	

	Visitors including other agencies Relatives Contractors	
12. Are you relying on individuals (patients/staff) to provide consent for the processing of personal identifiable or sensitive data?	No It is important to note that in principle there is no requirement to obtain the express consent of the person or persons being filmed since the actions of the security team are deemed to be lawful.	
13. If yes, how will that consent be obtained? Please state:	N/A	
14. Have the individuals been informed of and have given their consent to all the processing and disclosures?	Yes (explicit) Prior to any activation subjects and persons in the immediate vicinity will be informed of the activation by the operator. Immediately on the unit being turned on they will again be informed of its activation. Existing CCTV signage also includes the activation of BWV and privacy notices will be placed at all entry and exit locations to the hospital. • Any non-evidential material is retained for 31 days • This material is restricted and cannot be disclosed to third parties without the express authority of the subject of the recording unless prescribed by law; and • Recorded material is Trust information and that it can be accessed on request in writing in accordance with the GDPR & DPA, unless an exemption applies in the circumstances. The BWV operator will decide on a case-by-case basis when and when not to switch the BWV on or off. There should always be a presumption to record if the 'need to address a pressing staff/patient safety need' has been achieved unless the circumstances dictate otherwise	IGTK 203

15. How will the information be kept up to date and checked for accuracy and completeness?	Following a duty period and any activation the security officer will return the device to the security office (secure location, access controlled) and following a 'check-in' process they will 'dock' it into a dedicated port that automatically downloads all the captured information on the site manager's computer. This information cannot be deleted or altered and is encrypted. The officer will then identify the elements of captured data to be retained via the software and 'mark' the section appropriately. It will then be backed up on to the primary back-up and then secondary back-up if required. Once completed, the contents on the device are deleted and retained as stated. All other material will be automatically erased after 31 days. The security management team and site security manager will monitor for accuracy, completeness and being up to date.	
16. Who will have access to the information?	Trust security management team: • Head of Business Security • Business Security Specialist • Site Security Manager	
17. Do you intend to send direct marketing messages by electronic means? This includes both live and pre-recorded telephone calls, fax, email, text message and picture (including video)?	No	Privacy Check
18. If applicable, are there procedures in place for an individual's request to prevent processing for purposes of direct marketing in place?	N/A	Privacy Check
19. Is automated decision making used? If yes, how do you notify the individual?	No	Privacy Check
20. Is there a useable audit trail in place for the asset. For example, to identify who has accessed a record?	Yes Access to record strictly very limited to authorised personnel only (x3) and audit trail recorded via DEMS software.	IGTK 206
21. Have you assessed that the	Yes	

processing of personal/sensitive data will not cause any unwarranted damage or distress to the individuals concerned? What assessment has been carried out?	Full internal and public consultation and assessment completed:
	
	• Staff focus groups (200+ staff)
	• Barnsley Facilities Services (BFS)
	• Information Governance Department
	• Security Team
	• Business Security Unit
	• Head of Estates & Facilities
	• Director of Nursing & Quality
	• Trust Chaplaincy
	• Trust Volunteers
	• ICT Department
	• Equality & Diversity Advisor
	• Nursing Teams
	• Staff side representatives
	• Local Ward Alliance Party
	• Community Safety Group
	• South Yorkshire Police
	• Meadowhall Ltd
	• NHS England
	• BMBC
	• Local Councillors
	  ○ Cllr Roy Miller
	  ○ Cllr Jo Newing
	  ○ Cllr Clive Pickering
	  ○ Cllr Phil Lofts
	• G4S Security Solutions UK
	• NHS Professionals
	• Pogmoor Residents Association
	• Old Town Residents Association
	• Yorkshire Ambulance Service
	• South Yorkshire Fire & Rescue Service
	• NHS Barnsley Clinical Commissioning Group	

22. What procedures are in place for the rectifying/blocking of data by individual request or court order?	The procedures and principles applicable to BWV are similar to how the Trust handles requests or court orders for CCTV data. Issues relating to these requests will be referred to the Trust legal team and Director of Nursing and Quality. There is regular liaison between BSU and IG and	

	established meetings where requests are tabled and discussed. Any that appear problematic have a referral pathway.	
23. Does the asset involve new or changed data access or disclosure arrangements that may be unclear?	No Existing arrangements are in place for CCTV data access and disclosure and will remain unchanged.	SS PIA (12)
24. Does the asset involve changing the medium for disclosure for publicly available information in such a way that data become more readily accessible than before? (For example, from paper to electronic via the web?)	No Although BWV will now include audio data the medium will not be more readily accessible.	SS PIA (14)
25. What are the retention periods (what is the minimum timescale) for this data? (please refer to the Records Management: NHS Code of Practice)	BWV & CCTV – 31 days Data retained for evidential purposes – 3 years Data retained for safety purposes – 10 years	SS PIA (13)
26. How will the data be destroyed when it is no longer required?	Files permanently erased and all erasures monitored by security management team and Trust ICT.	IGTK 105
27. Will the information be shared with any other establishments/ organisations/Trust's?	Yes South Yorkshire Police Barnsley Metropolitan Borough Council Enforcement (rarely) Crown Prosecution Service Courts NHS England Other NHS Trusts Very occasionally, the media will be given footage or stills from BWV when the safety of staff, patients or public is at risk and that risk can be reduced.	IGTK 207
28. Does the asset involve multiple organisations whether public or private sector?	No Initial processing will be by contracted (G4S) staff only with asset always on site under secure	IGTK 207

Include any external organisations. Also include how the data will be sent/accessed and secured.	conditions. Asset will never be shared with contractor.	
29. Does the asset involve new linkage of personal data with data in other collections, or are there significant changes in data linkages?	No Video data also collected by Trust CCTV system but no direct linkage of systems. Building prosecution cases to support South Yorkshire Police may involve the creation of composite video evidence e.g. bringing together BWV and CCTV – thus seeking to present the available 'best evidence' of events for all those involved in establishing the truth.	SS PIA (8)
30. Where will the information be kept/stored/accessed?	Other – please state below: **Primary:** Passcode secure computer located in office with electronic access I/D and passcode access (personnel restricted). Office staffed 24/7 with only SIA security personnel and all visitors signed in and accompanied at all times. **Primary backup:** Secure remote drives, pass code protected. Pass code minimum of 15 digits Secure drives locked in secure cabinet when not in use. Access to cabinet personnel restricted. Secure cabinet located in office with electronic access I/D and passcode access (personnel restricted). Office staffed 24/7 with only SIA security personnel and all visitors signed in and accompanied at all times. **Secondary backup:** Secure remote drives, pass code protected. Pass code minimum of 15 digits held in government approved secure cabinet behind 3 locked doors, one of which is electronic monitored access control. This location in separate building approx. 200m from primary storage, access allowed by 2 members of security management team only.	IGTK 210
31. Will any information be sent off site	Yes	IGTK 208 & 308

If 'Yes' where is this information being sent	Further information: Footage will be supplied for evidential purposes only via encrypted data on sealed or password protected discs/drives. Footage must be requested by authorised police or local authority staff and collected by hand under signature. Immediate supply for life/death, detection of crime incidents will be provided in written request of a police officer of at least Inspector rank. In all cases a MG11 witness statement for continuity of evidence will be provided by site security manager. Master copy will be retained securely on-site.	
32. Please state by which method the information will be transported	Only by hand in <u>every</u> case.	IGTK 208 & 308
33. Are you transferring any personal and / or sensitive data to a country outside the European Economic Area (EEA)?	No	IGTK 209
34. What is the data to be transferred to the non EEA country?	N/A	IGTK 209
35. Are measures in place to mitigate risks and ensure an adequate level of security when the data is transferred to this country?	N/A	IGTK 209
36. Have you checked that the non EEA country has an adequate level of protection for data security? If yes, where?	N/A	IGTK 209
37. Is there a Security Management Policy and Access Policy in place? Please state policy titles.	Yes. Surveillance Camera Policy Security Policy Security Assignment Instructions (AIs)	IGTK 301 & SS PIA (11)
38. Has an information risk assessment been carried out and reported to the Information Asset Owner (IAO)? Where any	Yes – attached No significant collection, storage, handling, retention and destruction risks identified.	IGTK 301& Risk Ass

risks highlighted – please provide details and how these will be mitigated?		
39. Is there a contingency plan / backup policy in place to manage the effect of an unforeseen event? Please provide a copy.	• Trust Resilience Framework • Business Continuity Planning – BC-Lite • Assignment Instructions • Primary & secondary back-up of BWV data • Access denial procedures – security office	IGTK 301& Risk Ass
40. Are there procedures in place to recover data (both electronic /paper) which may be damaged through: **□ Human error** **□ Computer virus** **□ Network failure** **□ Theft** **□ Fire** **□ Flood** **□ Other disaster**	Yes. Data stored at two secure backup locations one within a separate building. Data stored on pass coded and encrypted remote drives all stand alone. • Human error – software support • Computer virus – stand-alone storage & ICT support • Network failure – emergency laptops (x4) + fall-back sites • Theft – Full procedure in place for theft of device • Fire – secondary backup location • Flood – secondary back-up location • Other disaster – BC plans & Resilience Framework	IGTK 301& Risk Ass
41. Is the PIA approved? If not, please state the reasons why and the action plan put in place to ensure the PIA can be approved	Yes No	
42. Is a full scale PIA required?	Yes No	

Form completed by:

Name: Mike Lees
• **Title: Head of Business Security**
Signature:
Date: 1 May 2019

Form Reviewed by:

• **Information Asset Owner (Name & Title): Mike Lees, Head of Business Security Unit**
Information Asset Administrator (Name &Title): Lisa Corbridge, Business Security Specialist

Information Governance Board Approval:

Name: Katie Hunter
Title: Head of Information Governance
Signature:
Date: 1st May 2018

Appendix – Glossary of Terms

Item	Definition
Personal Data	This means data which relates to a living individual which can be identified: A) from those data, or B) from those data and any other information which is in the possession of, or is likely to come into the possession of, the data controller. It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual
Sensitive Data	This means personal data consisting of information as to the: A) racial or ethnic group of the individual B) the political opinions of the individual C) the religious beliefs or other beliefs of a similar nature of the individual D) whether the individual is a member of a trade union E) physical or mental health of the individual F) sexual life of the individual G) the commission or alleged commission by the individual of any offence H) any proceedings for any offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in such proceedings

Direct Marketing	This is “junk mail” which is directed to particular individuals. The mail which are addressed to “the occupier” is not directed to an individual and is therefore not direct marketing. Direct marketing also includes all other means by which an individual may be contacted directly such as emails and text messages which you have asked to be sent to you. Direct marketing does not just refer to selling products or services to individuals, it also includes promoting particular views or campaigns such as those of a political party or charity.

Automated Decision Making	Automated decisions only arise if 2 requirements are met. First, the decision has to be taken using personal information solely by automatic means. For example, if an individual applies for a personal loan online, the website uses algorithms and auto credit searching to provide an immediate yes / no decision. The second requirement is that the decision has to have a significant effect on the individual concerned.
European Economic Area (EEA)	The European Economic Area comprises of the EU member states plus Iceland, Liechtenstein and Norway
Information Assets	Information assets are records, information of any kind, data of any kind and any format which we use to support our roles and responsibilities. Examples of Information Assets are databases, systems, manual and electronic records, archived data, libraries, operations and support procedures, manual and training materials, contracts and agreements, business continuity plans, software and hardware.
SIRO (Senior Information Risk Owner)	This person is an executive who takes ownership of the organisation’s information risk policy and acts as advocate for information risk on the Board
IAO (Information Asset Owner)	These are senior individuals involved in running the relevant service/department. Their role is to understand and address risks to the information assets they „own“ and to provide assurance to the SIRO on the security and use of those assets. They are responsible for providing regular reports regarding information risks and incidents pertaining to the assets under their control/area.
IAA (Information Asset Administrator)	There are individuals who ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management and ensure that information asset registers are accurate and up to date. These roles tend to be system managers

Implied consent	Implied consent is given when an individual takes some other action in the knowledge that in doing so he or she has incidentally agreed to a particular use or disclosure of information, for example, a patient who visits the hospital may be taken to imply consent to a consultant consulting his or her medical records in order to assist diagnosis. Patients must be informed about this and the purposes of disclosure and also have the right to object to the disclosure.
Explicit consent	Express or explicit consent is given by a patient agreeing actively, usually orally (which must be documented in the patient's case notes) or in writing, to a particular use of disclosure of information.

Anonymity	Information may be used more freely if the subject of the information is not identifiable in any way – this is anonymised data. However, even where such obvious identifiers are missing, rare diseases, drug treatments or statistical analyses which may have very small numbers within a small population may allow individuals to be identified. A combination of items increases the chances of patient identification. When anonymised data will serve the purpose, health professionals must anonymise data and whilst it is not necessary to seek consent, general information about when anonymised data will be used should be made available to patients.
Pseudonymity	This is also sometimes known as reversible anonymisation. Patient identifiers such as name, address, date of birth are substituted with a pseudonym, code or other unique reference so that the data will only be identifiable to those who have the code or reference.
Information Risk	An identified risk to any information asset that the Trust holds. Please see the Information Risk Policy for further information.
Privacy Invasive Technologies	Examples of such technologies include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining and logging of electronic traffic. Technologies that are inherently intrusive, new and sound threatening are a concern and hence represent a risk
Authentication Requirements	An identifier enables organisations to collate data about an individual. There are increasingly onerous registration processes and document production requirements imposed to ensure the correct person can have, for example, the correct access to a system or have a smartcard. These are warning signs of potential privacy risks.

Retention Periods	Records are required to be kept for a certain period either because of statutory requirement or because they may be needed for administrative purposes during this time. If an organisation decides that it needs to keep records longer than the recommended minimum period, it can vary the period accordingly and record the decision and the reasons behind. The retention period should be calculated from the beginning of the year after the last date on the record. Any decision to keep records longer than 30 years must obtain approval from The National Archives.

Records Management: NHS Code of Practice	Is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice. The code of practice contains an annex with a health records retention schedule and a Business and Corporate (non-health) records retention schedule.
General Data Protection Regulation	The Regulation define the ways in which information about living people may be legally used and handled. The main intent is to protect individuals against misuse or abuse of information about them. The principles of the Regulation are: Article 5 – Principles relating to processing of personal data Article 6 – Lawfulness of processing Article 7 – Conditions for consent Article 8 – Conditions applicable to child's consent in relation to information society services Article 9 – Processing of special categories of personal data Article 10 – Processing of personal data relating to criminal convictions and offences Article 11 – Processing which does not require identification
Data Protection Act	This Act defines the ways in which information about living people may be legally used and handled. The main intent is to protect individuals against misuse or abuse of information about them. The 8 principles of the Act state The

	fundamental principles of DPA specify that personal data must: □ be processed fairly and lawfully. □ be obtained only for lawful purposes and not processed in any manner incompatible with those purposes. □ be adequate, relevant and not excessive. □ be accurate and current. □ not be retained for longer than necessary. □ be processed in accordance with the rights and freedoms of data subjects. □ be protected against unauthorized or unlawful processing and against accidental loss, destruction or damage. □ not be transferred to a country or territory outside the European Economic Area unless that country or territory the rights and freedoms protects of the data subjects.
Privacy and Electronic Communications Regulation 2003	These Regulation apply to sending unsolicited marketing messages electronically such as telephone, fax, email and text. Unsolicited marketing material should only be sent if the requester has opted in to receive this information.