

SECURING HEALTHCARE -

A G4S ACADEMY PAPER



- 3 Executive Summary
- 4 Why is Securing Healthcare the Same - Only Different
- 5 What Needs Protecting?
- 7 The Challenges with Securing Healthcare
- 11 G4S Healthcare Security Services
- 13 Why Security and Facilities Together Don't Work
- 14 What Good Healthcare Security Looks Like
- 17 What to Look for in a Security Provider
- 20 Where to Start
- 21 Plan for the Future
- 22 Concluding Thoughts

Hospitals and healthcare facilities are some of the most active and dynamic public facilities.

Operating across multiple sites and large campuses with varied populations of patients, visitors and staff means that the job of securing healthcare is both diverse and complex - in an environment where spending needs to be tightly controlled.

A fit for purpose healthcare security plan should adequately cater for security provision across:-

- People
- Property
- Information
- Reputation

The plan should also address the common challenges faced by the sector including:-

- Car Park and Traffic Management
- Front of House Services
- Preventing Unauthorised Access
- Staff Abuse
- Alcohol and Drug Related Violence
- Theft of Drugs and Equipment
- Control Room management
- Missing and absconded patients

This paper highlights what “good security” looks like for the sector, together with what to look for in an outsourced security partner; and why a combined security and facilities service may not necessarily result in a more efficient operation.



**“This paper highlights what
“good security” looks like for
the healthcare sector.”**

WHY IS SECURING HEALTHCARE THE SAME - ONLY DIFFERENT?

By definition, healthcare is diverse and includes:

- Doctors
- Dentists
- Pharmacists

These sites typically do not operate with a permanent security presence, however the nature of the environments require professional security to:-

- **appease hostile or aggravated situations**
- **secure valuable or dangerous assets** such as medication
- **respond quickly** when properties are left vacant or unmanned, often in remote or rural locations
- **provide a permanent “eyes on”** what is happening on site

Healthcare also includes secondary care in local areas, principally made up of:

- planned hospital care
- rehabilitative care
- urgent and emergency care
- most community health services
- mental health and learning disability services

These facilities face common security challenges which need to be addressed, whilst balancing the need to provide an optimum patient experience.

The challenges include:

- **car park and traffic management** - the need to provide fast, clear and accurate information, a simple payment service, manage traffic flow and guide visitors to their destination and answer queries at a time when space is at a premium.
- **providing appropriate greetings** - often security are the first people that visitors see. Visitors need a comforting and informative greeting.
- **screening for unauthorised materials** - prevent inappropriate materials - alcohol, drugs, firearms from entering the campus.
- **incident response** - security needs a permanent “eyes on” in communal areas and car parks to provide a proactive service before incidents occur and deliver an appropriate response to deal with the situation.

The key challenge is to provide a safe environment for both patients, staff and visitors whilst providing the best possible experience for those that visit or work at the hospital /site.

“Provide a safe environment for patients, staff and visitors whilst providing the best possible experience.”

WHAT NEEDS PROTECTING?



Typically within healthcare, organisations will operate with a security plan that caters for security provision across:-

-  **People**
-  **Property**
-  **Information**
-  **Reputation**

This section discusses what content should be included for each area:-

People

Security should be committed to minimising violence and aggression in the Workplace and ensuring appropriate alerts are shared with employees about terrorist and other security risks.

Security should be responsible for ensuring that hospital staff are supplied with appropriate photographic identification and that access is strictly restricted and controlled.

Given the significant percentage of the workforce that operate alone or with vulnerable individuals, security should pay specific attention to ensuring that Trusts provide adequate levels of protection for this profile of workforce. This may include lone worker protection services or body worn CCTV for security.

Security should also be responsible for developing a Pro-Security culture in which employees feel able to challenge unknown people in their work area in order to support a safe environment for all.

WHAT NEEDS PROTECTING?

Property

Security should manage and minimise security risks to personal property owned by employees, visitors and patients by using a variety of methods. Methods may include:-

- Providing employees with somewhere secure to store their personal belongings whilst at work
- Establishing and maintaining a Patient Property and Lost Property Policy
- Limiting access to work areas to ensure that only those with authorisation can access the area or ward
- Maintaining a Trust Asset Register and carrying out asset audits
- Maintaining a Closed-Circuit Television (CCTV) as a preventative and protective measure
- Ensuring physical security is effective in preventing entry to unauthorised visitors
- Requiring departments to complete a regular Fire, Health and Safety (H&S) Checklist to identify any security hazards in the work area
- Completing an annual Security Risk analysis of all reported incidents to identify trends and determine any Trust assets that may be vulnerable to theft
- Developing a culture in which employees, agency/locum and students feel able to challenge 'tailgaters'
- Ensuring that portable Information Technology (IT) equipment and equipment in insecure areas is encrypted to make it unusable by unauthorised users, or in the event of loss or theft

Information

Security should work collaboratively with IT to issue and maintain a fit for purpose:-

- Data Security and Protection Policy
- Information Governance Policy

Reputation

Any negative impact on people, property or information resulting from a security breach could damage reputation, resulting in a loss of confidence from the general public in the ability to deliver adequate healthcare in a safe and secure manner.



This section explores some of the unique risks and challenges faced by the healthcare sector and how to confront them:

Car Park and Traffic Management

Often the first impression of a hospital is gained from the point when a patient or visitor parks their car. These car parks are often over populated, with a lack of space including insufficient capacity for staff, visitors and patients alike. Parking and outdated parking furniture such as poorly maintained barriers and pay and display machines can lead to unnecessary vehicle congestion, frustration and aggressive situations prior to the visitor even entering the hospital. Therefore, clear and dynamic signage is needed as well as overflow planning, together with a visible presence to calm and provide service to those who are subject to delays or frustration and ensure blue light services have immediate access.

Once the car is parked, the next challenge is payment. Any payment process needs to accept multiple payment methods, have a clear process for issuing a permit or ticket to park and also a continuity offering so that should equipment be inoperable, visitors retain an option to issue payment.

Within the car park environment, automation is a key subject. Automatic Number Plate Recognition (ANPR) and virtual parking permit solutions can be used to provide automated access to specific areas such as those reserved for staff and visitors. In these areas, cameras will recognise vehicle number plates and automatically provide access ie raise a barrier.

Car parking is not only a highly emotive subject for hospital estate managers, it also represents a significant source of valuable income that can be reinvested into the hospital's finances. With revenue to operating expense ratios of anywhere between 5-10:1, it is critical that a hospital's parking and traffic management is well managed.

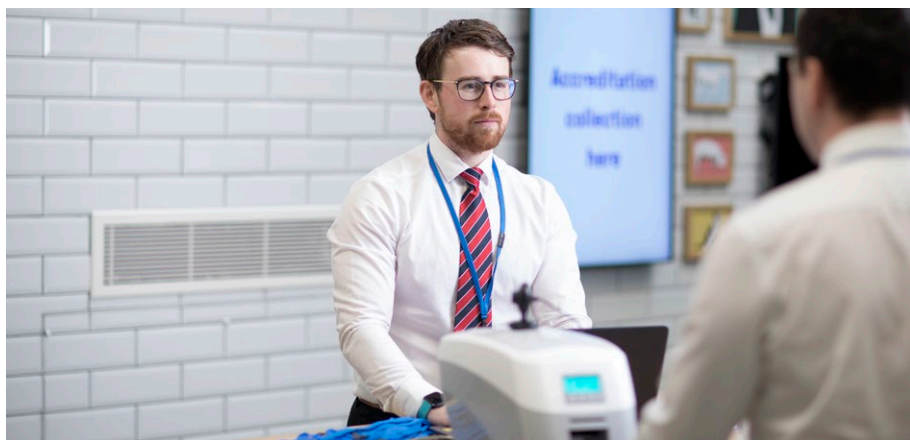


“It is critical that a hospital’s parking and traffic management is well managed.”

Front of House Services

The role of a security officer when situated at reception becomes more of a concierge service, in addition to providing eyes and ears to spot unwanted or suspicious behaviour and alert colleagues.

The officer will be required to signpost visitors, provide general customer service and be a friendly and professional representative for the hospital. It is therefore important for Healthcare Security Officers to be able to adapt their communication styles recognising that many visitors and patients may have impairments such as poor sight, speech or hearing, mental health or learning disabilities, dementia or other impediments.



“Often security is the first personal contact a visitor will have when entering a hospital.”

Preventing Unauthorised Access

Given the nature of the sites, restricting access is critical. In some high security sites not open to the public, this begins at the perimeter. Security will be required to patrol the perimeter at regular intervals and use technology to identify unusual activity or potential breaches before investigating.

Within hospitals, a fit for purpose access control system will prevent unauthorised access to secure areas such as those where drugs or expensive equipment are stored. The system should include a back end administrative software platform whereby staff permissions can be altered quickly and simply, to adjust the locations that staff are allowed to visit. This has been particularly valid during the Pandemic allowing hospitals to limit building ingress and egress, limiting the potential for spreading of COVID-19 and allowing enhanced people screening in designated areas.

The access management system should also alert or highlight suspicious activity - ie repeat visits to the same area or potential access breaches where an individual has gained access to an area in which they do not have the correct privileges.

Finally, in the highest security areas, the latest access technologies will use biometrics as a means of authentication. This could be used for a select group of staff to gain access to the highest value drugs or possibly IT infrastructure - any assets which require the highest level of protection.

Safety Incident Response

Within the hospital itself, security can also play a key role in incident response. As an example, fire marshalling, first responders or building evacuation. It is so important when an incident occurs that patient treatment time is not lost. Security officers can play a key role in freeing up medical staff to perform their core duties.

Staff Abuse

As the healthcare system comes under pressure, waiting times have increased. Patient frustration has grown in line - one Norfolk hospital has reported over 40 instances of staff abuse per month from frustrated patients and visitors, leading them to invest in private security to provide a safe environment for those carrying out their duties.

Incidents reported at the hospital have been primarily verbal including rudeness and sarcastic jeering and clapping which is said to be “upsetting and intimidating” for staff.

Recognising Signs of Mental Distress

For security officers themselves, it is so important that they are trained appropriately and carry the correct skills to recognise signs of mental distress. Hospitals are highly emotive environments where individuals - both patients, visitors and staff are subject to high levels of stress and an unpredictable reaction could occur at any time.

As a consequence, officers need to be able to recognise situations as they develop and then, in an aggravated situation, have the correct skills to de-escalate and calm the individual in question.

Alcohol and Drug Related Violence

Twelve to fifteen percent of A&E attendances are alcohol-related and over 1.1m hospital admissions each year have alcohol as a causal factor in the patient’s diagnosis. Newcastle NHS Trust report 914 incidents of physical or verbal assaults by patients, relatives or visitors in the twelve months to 30th June - up seventeen percent on pre-pandemic times - with alcohol and drugs a significant contributory factor.

Conflict resolution, de-escalation techniques, and restraint training are also essential skills for security staff, together with appropriate supporting equipment to deal with these situations as they occur.

Theft of Drugs and Equipment

Given the expensive nature of equipment and potential health issues of the drugs stored within hospitals, it is so important to have a fit for purpose access process to prevent theft and misuse. A number of cases have been reported in the press, including at Newcastle Freeman Hospital:

NEWCASTLE FREEMAN HOSPITAL PRESS REPORT

and Macclesfield General Hospital

MACCLESFIELD GENERAL HOSPITAL PRESS REPORT

Security can assist with the management of access control systems as well as using surveillance equipment to identify suspicious activity.

THE CHALLENGES WITH SECURING HEALTHCARE

Protecting Vulnerable Members of Staff

Most Trusts will operate with lone worker protection policies, designed to provide staff who operate alone or are vulnerable to attack with an adequate level of protection. Security have a key role to play with this profile of workforce. Technology may be provided which will deliver a permanent connection between the worker and security. In the event of a situation evolving, the staff member would be able to initiate a live connection with a security control room (either provided by the Trust or from a third party) which would diagnose the situation and organise a physical response, if required.

Securing Outlying Properties

Many primary healthcare facilities are located in rural locations and left unattended for long periods of time, despite them storing expensive equipment and potentially dangerous drugs.

Therefore, it is critical to maintain a relationship with an organisation that can permanently monitor for intrusion and provide a physical response when needed - against a firm service level commitment.

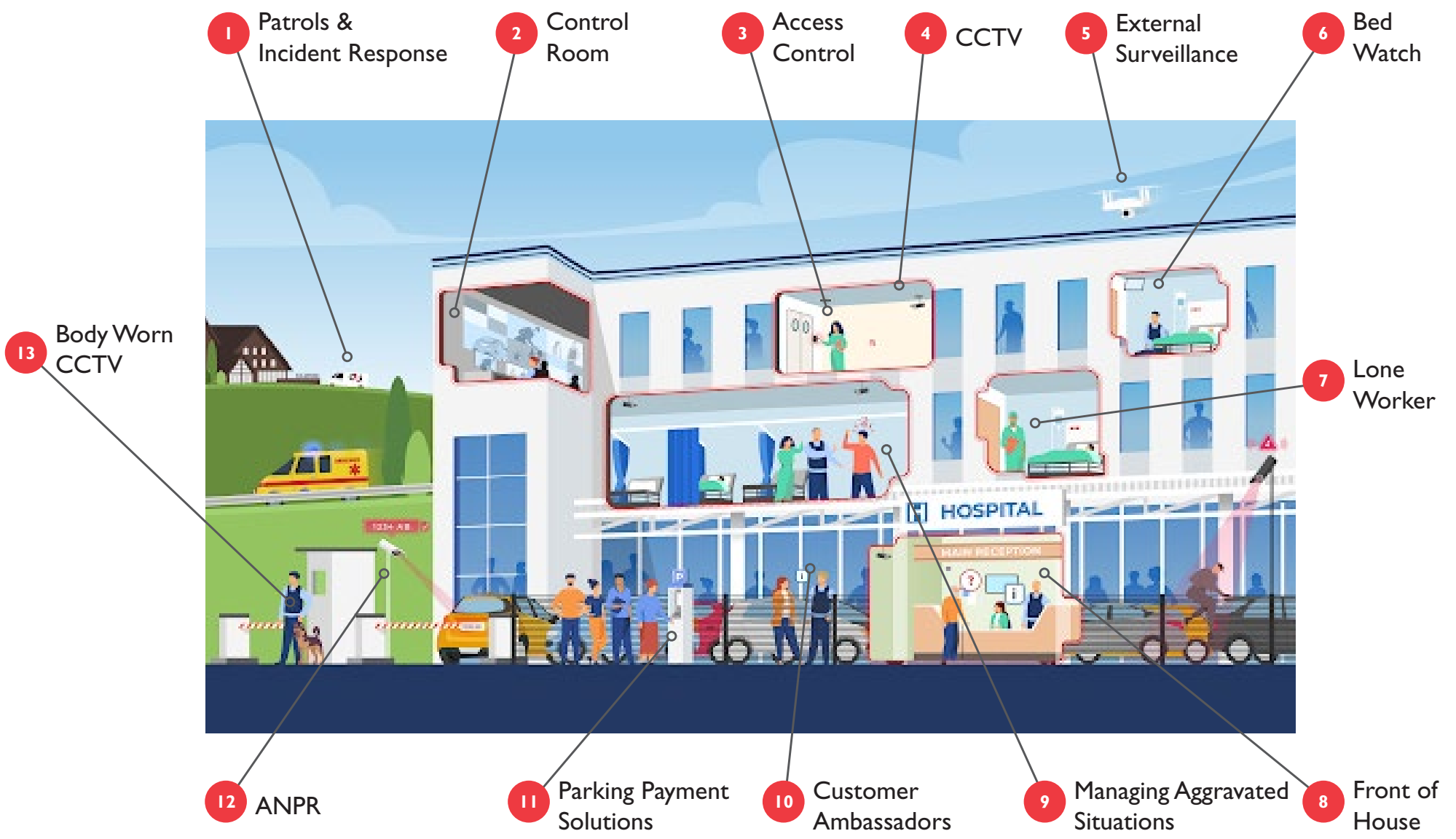
In addition, to comply with insurance premiums, a regular documented inspection will be required.

Short Term Demand - The Resource Challenge

For many Trusts, the security challenge can be one of short demand. Fluctuations in patient volumes and the need to keep COVID secure environments have left Trusts needing to resource large volumes of security on a short term basis. Therefore, each Trust should have a "Security Continuity" plan in place which provides "burst capacity" for situations where security is needed in volume, temporarily.



OUR HEALTHCARE SECURITY SERVICES



G4S HEALTHCARE SECURITY SERVICES

1. Mobile Guarding Response	<ul style="list-style-type: none"> For remote clinics or sites left unmanned, we provide a 24*7 intruder monitoring and surveillance service, supported by a physical site response whenever it is needed.
2. Control Room	<ul style="list-style-type: none"> We provide control room design services and the latest surveillance analytics to simplify the job of the control room operator and turn security into a proactive service.
3. Access Control	<ul style="list-style-type: none"> For sensitive assets such as drugs or equipment, we provide access control, including the latest biometric technology to restrict and monitor unauthorized access.
4. CCTV	<ul style="list-style-type: none"> We provide and maintain the latest surveillance technology with embedded analytics to alert to suspicious activity.
5. External Surveillance	<ul style="list-style-type: none"> We provide surveillance drones to provide external surveillance across campuses and large geographic areas, saving time over traditional external patrols.
6. Bed Watch	<ul style="list-style-type: none"> For particular circumstances where patients are a risk to themselves, or others, we secure the environment with a permanent physical presence.
7. Lone Worker	<ul style="list-style-type: none"> We provide lone worker services which provide a permanent connection between the lone worker and our monitoring station.
8. Front of House	<ul style="list-style-type: none"> Our staff provide a quality concierge service, to assist visitors and provide professional and courteous greeting to visitors.
9. Managing Aggravated Situations	<ul style="list-style-type: none"> Our staff are trained in advanced physical intervention techniques which can be common when dealing with patients and visitors under the influence of drink or drugs or who are suffering from poor mental health.
10. Customer Ambassadors	<ul style="list-style-type: none"> Our staff pride themselves on delivering the best possible customer service to become Ambassadors for your Trust or site.
11. Parking Payment Solutions	<ul style="list-style-type: none"> We provide payment collection technology to deliver a best in class parking experience – so important for busy healthcare trusts.
12. ANPR	<ul style="list-style-type: none"> To assist staff and regular visitors, we use ANPR technology to record vehicle license plates to ensure an optimum, secure parking experience.
13. Body Worn CCTV	<ul style="list-style-type: none"> Our bodyworn CCTV cameras provide an instant deterrent for the verbal and physical abuse that public-facing and frontline workers are often subjected to.

WHY SECURITY AND FACILITIES TOGETHER DON'T WORK

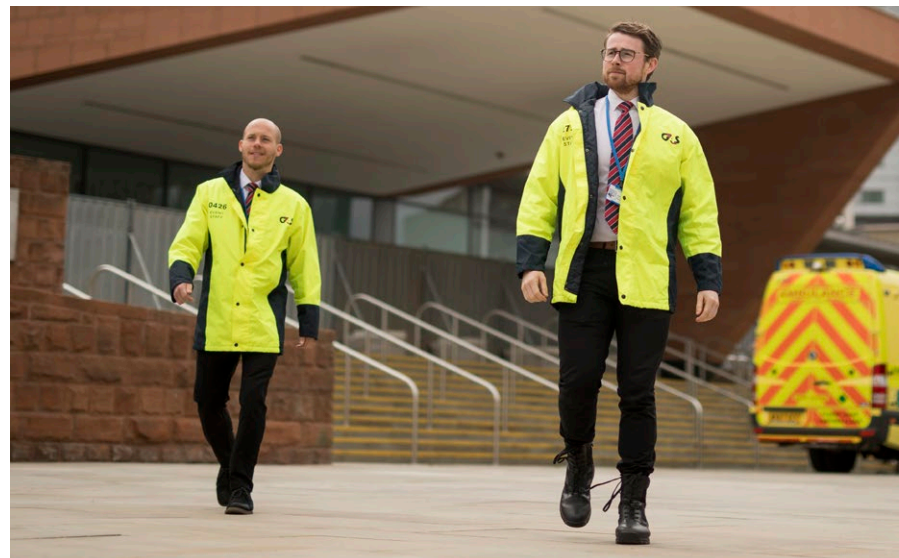
It is inherent upon any employer to meet their duty of care and offer the safest possible environment both to their employees and to anyone entering their place of work.

Healthcare professionals deserve the greatest level of protection as they serve their communities and those under their care. Hospital patients are in a vulnerable position during their stay and must also be afforded the correct levels of security from their caregivers and healthcare facilities. For these reasons, most hospitals take security issues very seriously.

Many healthcare provider organisations have implemented 'Total Facilities Management' strategies in the last decade or more. The attraction of these bundled services is the ability to blend the cost, management and administration of services, often high in human capital content and associated cost. 'Soft FM' categories such as cleaning, catering and portering are clearly of vital importance to the smooth running of hospitals. When Security is bundled with such FM services, however, the specialist focus and expertise that Security requires is all too often lost. This results in the Security service itself suffering in terms of quality.

The modern, professional security officer in a hospital requires diverse skills. One moment they may be required to recognise someone in an agitated or disturbed mental state and diffuse the situation. Moments later, they may be situated as the first person a new visitor sees when entering the hospital and be required to provide a warm and welcoming experience.

Healthcare Security officers require specialist training, support, management and a unique identity. Whilst, the bundling of services may provide convenience or - at first glance - a cost saving opportunity, the quality of service will suffer and in a high risk environment such as a hospital - the consequences can be very serious.



“For anybody entering into a hospital or a healthcare facility, security concerns should be the least of their worries.”

WHAT GOOD HEALTHCARE SECURITY LOOKS LIKE

Against this backdrop, it is important to identify and recognise “what good looks like” - here are some of the key items to look for when evaluating your security presence.

The Patient Experience

Consider whether your security officers are successfully striking a balance between reflecting a positive image of the hospital versus being expertly skilled in securing the hospital in the event of unanticipated disruption, violent act, or other emergency.

One of the most important characteristics of a good security program is that the security officers feel responsible for customer service and patient satisfaction. It is so important that security staff are trained in their hospital's particular culture and comfortable with regulations and legislation, in addition to being able to stand-down a perpetrator, curtail a domestic conflict or aggressive situation.

Fit for purpose healthcare security exists where security personnel serve as ambassadors of a hospital while ensuring the safety of patients, physicians, nurses, and staff. Can you really say that your security acts as ambassadors?

Situational Awareness

Situational awareness can be defined simply as “knowing what is going on around us”. Sounds simple, but in many healthcare sites, security is a reactive function, where officers work independently and by the time they respond to incidents, it is simply too late.

Good healthcare security embeds technology, to allow control rooms and officers to collaborate so that by the time the officer arrives on the scene, she or he is equipped with the correct visibility and information to provide an appropriate response.

Training and Education

It is so important that the security officers deployed across the Trust have the correct skills and are trained appropriately in order to carry out their duties. Are your security officers appropriately skilled to:

- Recognise signs of mental distress
- De-escalate hostile or aggravated situations
- Intervene in a crisis
- Provide “last resort” physical response
- Act as customer ambassadors for patients and visitors
- Respecting equality and diversity

It is critical that an appropriate continuous learning programme is in place and that officers can demonstrate the skills required to handle situations that present themselves on a daily basis across a busy Trust. Being appropriately skilled is a continuous activity as threats continuously evolve.

“The security officers feel responsible for for customer service and patient satisfaction.”

WHAT GOOD HEALTHCARE SECURITY LOOKS LIKE

Integration in Action

Does your security technology and personnel provision operate as one? Good security should evaluate risk and adopt a holistic approach, combining personnel, operational technology (communication devices), access management and CCTV.

Only by adopting a holistic approach to security will you ensure that your security is appropriate for your budget, appetite for risk and that services come together to ensure the best possible response when a situation occurs.

Contingency Plan

Many Trusts find themselves in situations where large volumes of staff are required at short notice. Challenge your security provider to evidence that they can provide high volumes of staff at short notice so that you can be confident of delivering continuity of service in an emergency, or burst capacity should increased security be required at short notice.

Monitor and Measure

Does your security provider deliver appropriate management information which demonstrates performance against contracted service level agreements? Is this data valid and usable? Are they delivering on their promise? If the answer is that you are not sure - it is time to review.

Threat Intelligence

How proactive is your security partner? Do they provide you with threat intelligence that will prepare you for times when terrorist or other threats are heightened? If the answer is no, challenge them to provide proactive information to turn security from a reactive to proactive function.

Do you Operate a Pro-Security Culture?

Developing and sustaining an effective Pro-security culture is an essential component of a protective security regime, and helps mitigate against a range of threats that could cause physical, reputational or financial damage to organisations. It is the responsibility of your security team and leadership team to embed this culture.

Security culture refers to the set of values, shared by everyone in an organisation, that determine how people are expected to think about and approach security. Getting security culture right will help develop a security conscious workforce, and promote the desired security behaviours you want from staff.

Consider carefully, whether your provider is making adequate effort to embed such a culture within your Trust. If they are not, it may be time to act.



WHAT TO LOOK FOR IN A SECURITY PROVIDER

So, now we have referenced what to look for from your existing security partner or function, here's some areas to challenge any prospective new partner:

A Track Record

Find a partner that can evidence a presence within healthcare and can provide a reference for the services that they provide.

Challenge them to demonstrate training programmes that will equip officers with the correct skills to deliver the services that you require.

Finally, work collaboratively with procurement to validate that the prospective partner carries the appropriate accreditations within the sector to facilitate a simple procurement process.

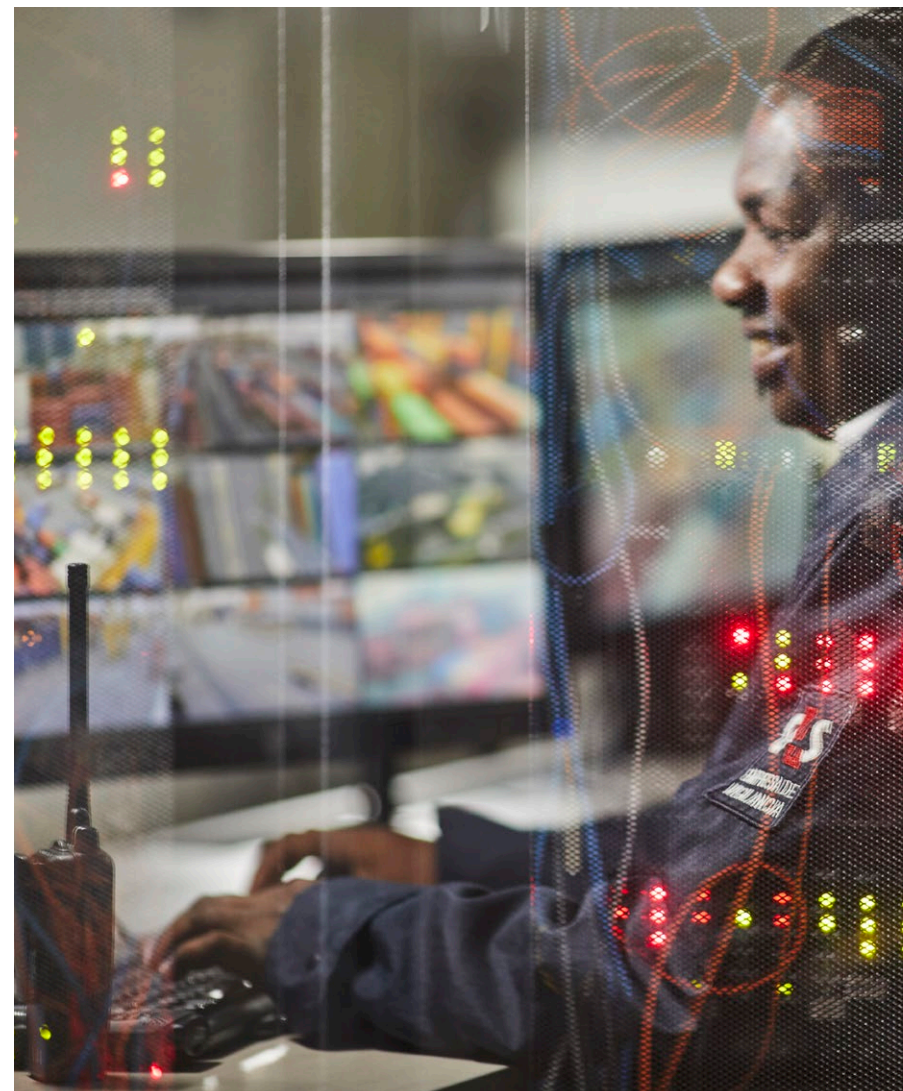
Technology Capability

Better security relies on better information which relies on better technology. Situational awareness, full site surveillance, operational communication and access management are all reliant on effective communication.

It makes it so much simpler if your security provider has their own technology portfolio. It simplifies your supply chain, leads to savings and places clear accountability in the hands of the security provider.

A Training Programme

Finally, we've referenced throughout this paper, the skills needed to deliver security effectively within healthcare. It is critical that your provider can evidence a training programme that equips officers with the correct skills to be effective.



The Process of Managing Change

Should you be considering outsourcing, it is so important to choose an organisation with a demonstrable track record in providing professional security services for organisations based across the United Kingdom.

As well as the provision of the services, the provider should be required to demonstrate their competence in transferring staff into their ownership without causing disruption or significant churn.

This process is known as “TUPE”. TUPE stands for the Transfer of Undertakings (Protection of Employment) Regulations, which are rules that were introduced to protect employees when the business they are employed by changes hands. This includes when a company chooses to outsource or make a “service provision change”, such as moving to use an external security provider.

The regulations ensure that any liabilities employees have with their original employer are transferred to the new employer. For example, employment rights and benefits such as bonuses and annual leave allowance.

In simple terms, this means that when we take on existing staff, we work in line with the regulations to honour their current employment package.

Whilst many of our customers are keen to transition away from an in house provision, they are justifiably concerned about the potential impact it may have on their security team and their ability to provide continuity of service.

While most believe outsourcing their security will help raise standards and boost cost-efficiency, they are worried their existing officers simply won't like it.

It is critical that the “receiving security provider” has adequate TUPE and induction procedures and creates a positive culture immediately. Here is some information on what you should expect.

The receiving provider should:-

- Meet each officer individually to talk them through the process, learn more about them and discuss any issues or concerns they may have.
- Confirm individuals' experience and the training they have received to date.
- Assess their ability to undertake the work to an acceptable standard
- Complete a comprehensive onboarding process, which should include an introduction to their culture, business goals and code of conduct
- Discuss other opportunities that may exist within our business and to hear what their individual development goals and ambitions may be
- Undertake regular managerial and supervisory visits to ensure all staff feel included
- Have appropriate communication vehicles to ensure all staff receive company content

“Demonstrate competence in transferring staff without disruption or churn.”

Provide a Business Case

Most outsourced processes start with a business case which outlines the rationale for change whether that be service improvement, cost saving etc. Once approval has been met, initiate an outsourcing process and a project team can be created.

The Project Team

Outsourcing is essentially a project and needs to be run like one with a project plan, communication plan and clear project governance. Make sure the work is properly resourced with people who have the time, expertise and authority to move the process forward.

Create the Tender

If a convincing business case is put together and the decision is taken to go ahead with outsourcing, then the next stage will be dictated by your procurement process. Different Trusts will have their own arrangements, but there are some consistent requirements:

- Be clear on how you want to approach the tendering process — do you want security providers to provide innovative proposals or respond to a prescriptive brief?
- Write a clear tender that includes as much information as possible to allow the respondents to provide an accurate response
- Think carefully about performance standards and service levels
- Be aware that managing vendors, reviewing tenders and evaluating returns is a time-consuming process. Make sure that the people in the team have the time to dedicate to the project

- Ensure that when evaluating tenders, there is a clear framework and scoring card. Any decision made needs to be reasoned, have a clear audit trail and be justifiable

Once tenders are submitted, evaluate them against the business plan and original objectives — do they meet the criteria first outlined?

Making sure that you are clear from the outset about what you want and what your priorities are, it will make this phase significantly easier. It will also help ensure that you lead the negotiations, rather than being led by the vendor.

At all times keep senior management informed — ultimately they'll be required to sign off on any deal, so it's important they know where discussions are headed.



Managing Transition

Once you have identified your preferred vendor, there will be a transition phase whereby services, knowledge and assets are transferred to the new provider.

Managing expectations, a clear governance structure and regular communication is absolutely critical at this stage. A good contract will help, but the relative performance of many contracts can lie in the relationships between the respective managers on both sides of the agreement.

Developing a truly collaborative, trusting relationship will be fundamental to both tackling problems early on, and establishing a good base for the future.

Managing Performance

Once the contract is fully mobilised, ensure that your new provider has adequate systems and processes in place to provide full and transparent management information, allowing you to assess their performance against the contract key performance indicators.

“Assess performance against key performance indicators.”



It is so important to have a clear vision of the skills and equipment to deliver security in the future and to be working towards achieving this goal.

Simply, delivering security in the way it has always been delivered, will result in security that is no longer relevant, is ineffective and is likely to result in a poor representation of your Trust. So what should the future of security in healthcare look like?

Moving forwards, healthcare security should:

Be Diverse

Security should be made up of diverse gender and ethnic backgrounds representative of the Service User community and also, importantly, show a respect and understanding for other cultures.

Have the Appropriate Skills

Security should maintain diverse skills to be effective in healthcare - from recognising signs of mental distress to appeasing aggravated situations, to front of house customer service and more.

Be Multi Disciplined

Security should be multi disciplined to combine customer service with traditional security, be first responders for fire and other safety incidents and also be prepared to work collaboratively with facilities to undertake a broader suite of tasks.

Operate with Transparent Performance Indicators

Security should be enabled with operational technology that records key performance information such as patrols, inspections and incident

responses in one or multiple locations and consolidates the data for easy to consume analysis. This will allow the measurement of performance against contracted SLA's.

Be Situationally Aware

Security should combine real time surveillance using intelligence to identify suspicious or unusual behaviour, with operational technology such as handhelds to ensure that when an officer arrives on the scene, they are in constant communication with the control centre and equipped with the correct information to provide an appropriate response.

Embrace Technology

Security should embrace surveillance and modern access methods to allow them to become an intelligent proactive function. Modern surveillance will provide artificial intelligence which will draw attention to unusual or suspicious events, such as vehicles speeding or individuals accessing locked down areas.

Continuously Evolve and Improve

The needs of hospital Service Users and the estate itself are constantly evolving and the Security service provision should be a reflection of this. Using Penetration Testing, Mystery Shopper techniques, surveys and of course periodic more formal reviews in the form of a Security Risk Assessment will allow for gaps and vulnerabilities in the Security solution to be identified and appropriate measures taken. Pro-active ideas and innovation to drive improvements in Security operations should be part of the Security service DNA to strive for improved outcomes meeting the needs and objectives of the Trust.

CONCLUDING THOUGHTS

Clearly, it is critical to identify a security provider that can evidence an understanding of the bespoke requirements of the security, supported by a successful track record of delivering services to healthcare and a commitment to CPD.

The G4S Academy provides regular networking opportunities, threat intelligence and thought leadership material.



Our G4S Academy providing a monthly security bulletin on potential as well as a repository of white papers, webinars and other continuous professional development material



Our Events and Seminars where guest speakers debate the latest market evolution and trends



Our Innovation Forum where we work closely with our customers to discuss new security issues and how best to address emerging trends and technologies



Our Podcasts where we support continuous professional development through engaging debate - available at your leisure



Listen to Noah's introduction and subscribe with our G4S Academy for free at <https://www.g4s.com/en-gb/what-we-do/academy>





Contact Us

UK: 08459 000 447
enquiries@uk.g4s.com

2nd Floor, Chancery House,
St. Nicholas Way,
Sutton,
Surrey,
England, SM1 1JB

Ireland: 1890 447 447
g4ssales@ie.g4s.com

