Req No	Description	Level 1 Summary of Requirements	Level 2 Summary of Requirements	Care Home Comments
Information Governance Management				
114	Responsibility for Information Governance has been assigned to an appropriate member, or members, of staff	Named & Trained IG Lead and Lead clinician/care professional Evidence: An email to a staff assigning responsibility, Certificate of attendance to training or amend job description. Most organisations already have IG leads/Quality lead	Current IGT Assessment & Improvement Plan	May find IG specific policy and IG training for those with a key role are required NHS Mail considerations: • This should include a named contact for NHS Mail within the organisation
115	There is an information governance policy that addresses the overall requirements of information governance	Staff have access to full range of required policies and procedures but these have not been agreed by the management team Action: create new policy or review current one and adapt if required. Get approval from management.	Staff have access to full range of required policies and procedures agreed by the management team	May find that you have some existing policies but may need reviewing and acknowledge as part of IG framework. NHS Mail considerations: • ICT Policy and Procedures • Mobile Device Policy • Information Sharing Policy
117	All staff members are provided with appropriate training on information governance requirements	Majority of staff have been trained on IG basics as required by role. Update induction plans to include IG training to Home training matrix so that this is annually updated for all staff, volunteers/agency and student workers.	All staff have been trained on IG basics and induction for new staff includes IG training	May find existing training may support this requirement. Check against the requirement first and consider your policies and procedures within your IG Framework. Use this link https://www.igtt.hscic.gov.uk/igte/index.cfm and follow the 'Take the guest tour' for access to some training material
Confidentiality and Data Protection Assurance				
202	Confidential personal information is only shared and used in a lawful manner and objections to the disclosure or use of this information are appropriately respected	Plan for ensuring all confidential data usage or sharing has a legal purpose. Update confidentiality policy and reference new information pack. Policy should be signed off.	All flows and uses of confidential personal information have been identified and documented with a legal basis	May find that you have some information that address this requirement but don't have a single flow mapping register for the whole organisation. NHS Mail considerations: • Users must also agree to the NHS Mail Terms of Use. This is part of the NHS Mail account registration process.

Req No	Description	Level 1 Summary of Requirements	Level 2 Summary of Requirements	Care Home Comments
213	There is a publicly available and easy to understand information leaflet that informs patients/service users how their information is used, who may have access to that information, and their own rights to see and obtain copies of their records	Basic information about the use of personal data is made available to service users via a leaflet. Update your pack to show info about NHS.net. Get approval. Template in USB.	Staff have been informed about the communication material and there is more comprehensive information available to service users that require it	May find you already provide sufficient information to patients / service users but check against the guidance. NHS Mail Considerations: • Organisation procedures and material should be updated to reflect use of NHS Mail
Information Security Assurance				
316	There is an information asset register that includes all key information, software, hardware and services	The Care Home has a comprehensive register of its information assets. Update JD to show who's role to update asset register.1	All information assets have been risk assessed and steps taken to ensure they are secure	May find that you have some information that address this requirement but don't have a single Information Asset register for the whole organisation. NHSmail Considerations: Assess the use of NHSmail and any impacts on information risk
319	There are documented plans and procedures to support business continuity in the event of power failures, system failures, natural disasters and other disruptions	There has been an assessment of the risks to all systems where information critical to the running of the organisation is held. The asset register will identify any business critical assets; these might be available at other homes or back up plans for manual reasons would be in place. This should be referenced in the BCP.	There is a business continuity plan that has been approved by senior management. All staff are aware of their roles and responsibilities.	May find you already have this material in place but check it against the guidance and ensure this is kept up to date. NHS Mail consideration: • Business Continuity Plans should cover alternative processes in the event NHS Mail is unavailable.

Req No	Description	Level 1 Summary of Requirements	Level 2 Summary of Requirements	Care Home Comments
320	There are documented incident management and reporting procedures	Responsibility for leading on the management and reporting of information incidents has been assigned to an appropriate member of staff. Evidence: Update JD to reflect. Remind staff in meetings and update. Make sure this is an agenda for meetings.	Incident management and reporting procedures have been implemented and staff have been informed of how to report incidents and near-misses.	May find you already have these procedures in place but should reviewed against the guidance to make sure any IG specifics is included. NHS Mail considerations: • Procedures should include reporting security incidents to NHS Mail Helpdesk e.g. phishing emails. • If you utilise an IT support company consider if this should be part of their reporting processes.
325	Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely	Responsibility for network security has been assigned to an individual who undertakes reviews of information security risks.	The approved controls and procedures for network security in respect of all ICT networks controlled by the organisation have been implemented.	IG Toolkit can be marked as **Not Relevant** if ICT networks are not controlled by the organisation. Note: This applies to the systems and applications using the network as well as the information passing through it. NHS Mail considerations: • Procedures are reviewed to ensure Antivirus / malware software is kept up to date and overall status reported on.